HOUSE OF COMMONS
CANADA

STATUTORY REVIEW OF THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics

Tom Wappel, MP
Chairman

May 2007

39th PARLIAMENT, 1st SESSION

Also available on the Parliamentary Internet Parlementaire: http://www.parl.gc.ca

Available from Communication Canada — Publishing, Ottawa, Canada K1A 0S9

STATUTORY REVIEW OF THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics

Tom Wappel, MP
Chairman

May 2007

39th PARLIAMENT, 1st SESSION

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIRMAN

Tom Wappel

VICE-CHAIRMEN

Pat Martin

David Tilson

MEMBERS

Sukh Dhaliwal

Glen Pearson

Scott Reid

Dave Van Kesteren

Mike Wallace

Carole Lavallée

Jim Peterson

Bruce Stanton

Robert Vincent

CLERK OF THE COMMITTEE

Richard Rumas

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Kristen Douglas

Nancy Holmes

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

FOURTH REPORT

Pursuant to its mandate under Standing Order 108(2), the Committee has studied a Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA) and agreed to the following report:

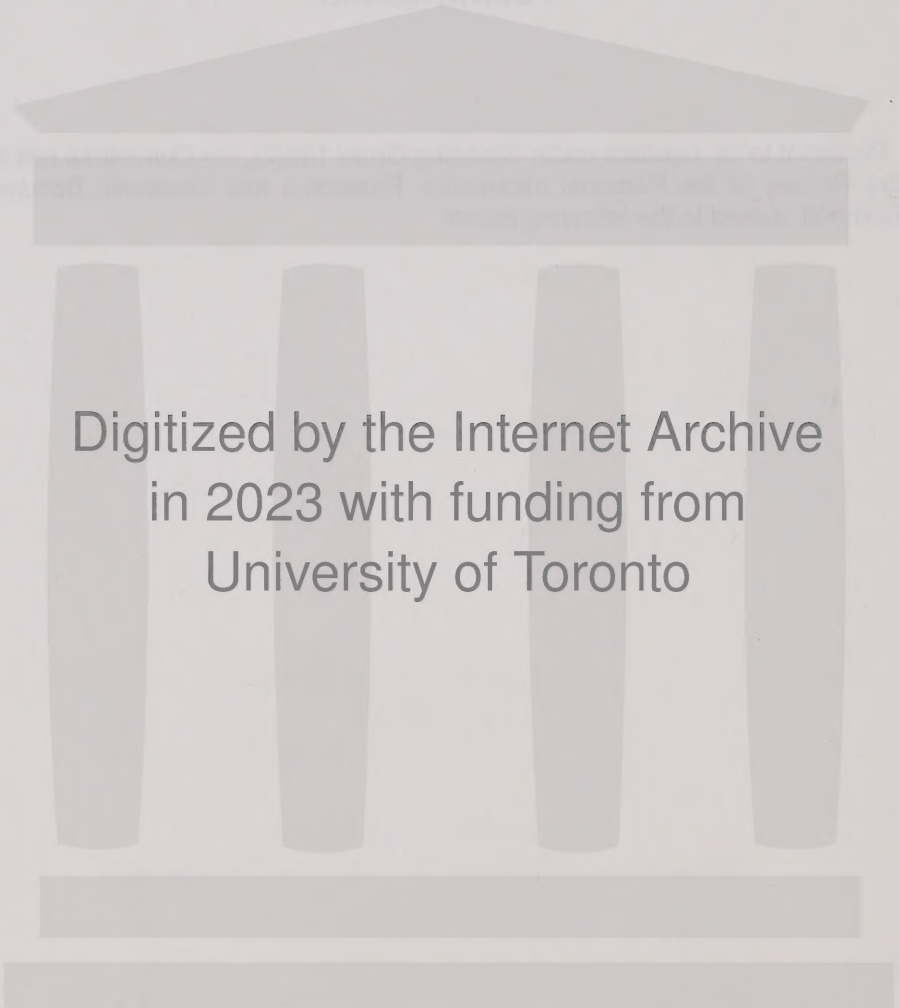

TABLE OF CONTENTS

INTRODUCTION

Pursuant to section 29 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and an order of the House of Commons, the Standing Committee on Access to Information, Privacy and Ethics (the Committee) held hearings on the administration of Part 1 of the Act, Protection of Personal Information in the Private Sector. The Committee heard from 67 witnesses between November 20, 2006 and February 22, 2007 and received 34 submissions from additional individuals and organizations.

All of our witnesses were generally supportive of a federal private sector data protection law, particularly in view of the rapidly expanding myriad of information technology and its ability to transcend national borders. In this context, the crux of the debate before us was how best to maintain the balance sought by the legislation in terms of protecting the privacy rights of individuals (what is known about them and by whom) and the legitimate needs of business organizations to manage their information holdings.

This report does not advocate dramatic changes to PIPEDA at this time. Given that the full implementation of the Act did not come about until January 2004 (see Overview of the Act, below), the Committee is cognizant of the fact that not every aspect of its implementation has yet been fully realized. Thus, even though we heard arguments on numerous issues, we have addressed only those where we decided that comments are warranted at this time.

The recommendations in this report essentially seek to provide some fine-tuning, much of which is premised on the need for greater harmonization between PIPEDA and the provinces of Quebec, Alberta and British Columbia, all of which have substantially similar private sector data protection laws. Indeed, we heard from privacy advocates, academics, business and industry organizations, as well as from the Federal Privacy Commissioner, that reference should be made to these provincial laws when making changes to PIPEDA. In particular, it was argued that the Alberta and British Columbia laws, having been drafted subsequent to the Quebec and federal Acts, have had the benefit of drawing upon the Quebec and federal experiences and incorporating enhancements to their legislation. It was argued that these "second generation" privacy laws provide a more practical and updated reflection of privacy protection today.

We recognize that there is a need to devote more resources to the education of both individuals and organizations about their respective rights and responsibilities under PIPEDA. We heard evidence that most Canadians are unaware of their privacy rights in general, let alone those with respect to PIPEDA. We also heard that one of the biggest challenges for most small and medium businesses is to understand their obligations under the law. In our view, the success of any amendments we propose to PIPEDA, and ultimately of PIPEDA itself, will depend on individuals being able to make informed choices

about their personal information and organizations being fully aware of their obligations under the Act. Given that the Office of the Privacy Commissioner has a clear mandate to foster public awareness and encourage compliance amongst organizations subject to the legislation, we hope that more work will continue to be done in this area and that the government, for its part, will also work with both organizations and the Privacy Commissioner to this end.

OVERVIEW OF THE ACT

Subject to certain statutory exemptions,[1] PIPEDA applies to private sector organizations that collect, use or disclose personal information in the course of commercial activities. It also applies to the collection, use and disclosure of personal information pertaining to the employees of federally regulated organizations.[2] Personal information is broadly defined (section 2(1)) as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." Obviously intending to capture a broad range of transactions, section 2 of PIPEDA defines "commercial activity" as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."[3]

PIPEDA has come into effect in three stages:

- On January 1, 2001, the Act applied only to the federally regulated private sector (i.e., telecommunications, broadcasting, banking and interprovincial transportation and airline industries). It also covered interprovincial or international trade in personal information.

- On January 1, 2002, personal health information became subject to the Act.

---

1 The Act does not apply to any government institution to which the federal *Privacy Act* applies; to personal information collected, used or disclosed by an individual exclusively for personal or domestic purposes; or to organizations in respect of personal information that is collected, used or disclosed for journalistic, artistic or literary purposes (s. 4(2)).

2 Notwithstanding provincial jurisdiction over labour relations, the federal government can regulate employee information but only in relation to works, undertakings and businesses that are within the legislative authority of the federal Parliament.

3 PIPEDA is limited in its scope to commercial activities because the provinces have exclusive jurisdiction over matters of private property and civil rights. The federal government therefore chose to regulate this area based on its general power to regulate trade and commerce.

- On January 1, 2004, the provisions of the Act extended more broadly to include all organizations located entirely within a province, even if they collect, use or disclose personal information only within that province. Where, however, a province enacts legislation that is substantially similar to the federal law, organizations covered by the provincial legislation may be exempted from the application of the federal Act. To date, only Quebec, Alberta, Ontario (with respect to personal health information) and British Columbia have provincial legislation that has been accorded the status of substantially similar to PIPEDA.

Once an organization falls within the scope of PIPEDA, section 5 requires that it comply with the fair information obligations set out in the Canadian Standards Association (CSA) Model Code (Schedule 1 of the Act)[4], unless the exceptions contained in sections 6 to 9 apply. Section 5 also provides that the use of the word "should" in Schedule 1 indicates a recommendation and does not impose an obligation. Section 5(3) of the Act further stipulates a "purposes" test by stating that the purposes for which an organization can collect, use or disclose personal information are to be limited to those that "a reasonable person would consider are appropriate in the circumstances." Section 7 of the Act sets out a number of exemptions pursuant to which an organization can collect, use or disclose personal information without the knowledge or consent of the individual and as such, is critical to the operation of the Act's privacy regime.[5]

PIPEDA provides individuals with a right to have access to their personal information and to have it corrected, if necessary. An organization must respond to a request for access within 30 days, but can extend this time limit under certain conditions; it can refuse to give an individual access to his or her personal information where this would reveal personal information about a third party and the third-party information cannot be severed from the record. If the third party consents, however, or if the individual needs the information because his or her life, health or security is threatened, the third-party prohibition will not apply. Furthermore, an organization can refuse to give access to

---

4 In response to the lack of national data protection standards in Canada in the early 1990s, a committee of consumer, business, government and labour representatives developed, under the auspices of the Canadian Standards Association (CSA), a set of privacy protection principles that, in 1996, were approved as a national standard by the Standards Council of Canada. The CSA *Model Code for the Protection of Personal Information* comprises ten interrelated privacy principles that were designed to serve as a fair information practices guide that could be adopted by businesses. The text of the CSA Code was ultimately incorporated into PIPEDA as a Schedule to the Act. For more on the origins of the Code and its adoption into PIPEDA, see *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* by Perrin, Black, Flaherty and Rankin, Irwin Law Inc., Toronto, 2001.

5 For example, personal information may be *collected* without the knowledge or consent of an individual for law enforcement purposes; when the collection is in the best interests of the individual; when the collection is for journalistic, artistic or literary purposes; or where the information is publicly available. Personal information may be *used* without the knowledge or consent of an individual for similar reasons, as well as for research purposes in certain instances with the knowledge of the Privacy Commissioner. Finally, personal information may be *disclosed* without the knowledge or consent of the individual for law enforcement and national security purposes, emergency situations, as well as research or archival purposes.

personal information where the information is protected, for example, by solicitor-client privilege or where access to the information would reveal confidential commercial information.[6] Access is permitted, however, if the individual needs the information because his or her life, health or security is threatened.

PIPEDA is administered pursuant to an ombudsman model similar to that found in the *Privacy Act* and the *Access to Information Act*. Individuals may complain to the Federal Privacy Commissioner about an organization's compliance with the legislation or the CSA Code[7], and the Commissioner will usually attempt to resolve the matter through persuasion and negotiation. Where this approach does not work, the Commissioner has the power to summon witnesses, administer oaths and compel the production of documents in order to render a finding in the matter. This finding must be set out in a report by the Commissioner within one year of the filing of the complaint. The Commissioner's findings are not binding on the parties, nor do they have persuasive value before the Federal Court. The complainant, after receiving the Commissioner's report, does however have the right to seek judicial remedies, including orders to comply and damages, from the Federal Court.

The Privacy Commissioner also has the power, under section 11 of the Act, to initiate her own complaints when she is satisfied that there are reasonable grounds to investigate a matter under the law. The Commissioner may apply to the Federal Court for review of complaints she has initiated as well as on behalf of a complainant with his or her consent. Pursuant to section 18 of the Act, the Privacy Commissioner also has the power to audit the personal information management practices of an organization where the Commissioner has reasonable grounds to believe that the organization is contravening the provisions of the legislation pertaining to the protection of personal information, or is not following a recommendation set out in the CSA Model Code.

Section 28 of PIPEDA creates offences for obstructing the Commissioner in an investigation or an audit, destroying records that are the subject of an access request before all recourse under the Act is exhausted, or dismissing, suspending, or demoting an employee who discloses a violation of the Act by his or her employer.

---

6 These access exemptions largely mirror those found in the *Access to Information Act* and are an example of the complementary nature of the privacy and access regimes.

7 Section 11.

DEFINITIONS

1. Personal Information

A. Business Contact Information

Section 2(1) of PIPEDA defines "personal information" for the purposes of the Act as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." Thus, business contact information is excluded from privacy protection in order that customers and others can easily communicate with the employees of organizations. Similar provisions are found in the federal *Privacy Act* with respect to public servants.

We heard from several organizations that the exclusion of business contact information under the Act should be broadened in order to recognize the current realities of how businesses communicate with their customers. It was suggested that a definition of "business contact information" be included in the Act to include all relevant types of information that are given out in a business context, and that the definition not be tied to any specific technology. Thus, business contact information should include business email and fax numbers as well as other similar business information.

The Privacy Commissioner directed the Committee's attention to the approach taken in the Alberta *Personal Information Protection Act*. The Commissioner liked the definition in this second general privacy law because it is sufficiently broad, but it also places restrictions on the purposes for which such information may be collected, used or disclosed.

Section 1(a) of the Alberta Act defines "business contact information" as an "individual's name, position name or title, business telephone number, business address, business email, business fax number and other similar business information." Section 4(3)(d) of the Act is the exception provision that states that the Act does not apply to business contact information where it is collected, used or disclosed for the purposes of contacting an individual in that individual's capacity as an employee or an official of an organization, and for no other purpose.

This Committee feels that business contact information should be excluded from PIPEDA's privacy protections and that what constitutes such information should not be tied to the information technology that exists at a particular point in time. The Act should therefore be updated to include business email and fax numbers, as well as future innovations in business communication. Like the Privacy Commissioner, we prefer the Alberta approach to this issue and make the following recommendation.

Recommendation 1

The Committee recommends that a definition of "business contact information" be added to PIPEDA, and that the definition and relevant restrictive provision found in the Alberta *Personal Information Protection Act* be considered for this purpose.

B. Work Product

The distinction between what is personal information about an individual, as opposed to information generated as a result of professional, business or employment activity, and its explicit recognition in PIPEDA, was a point raised by employers, businesses and health information providers. Many businesses are concerned about the effect on innovation and economic growth if workers are able to treat data about their work output or business strategies as personal information under PIPEDA. Mark Yakabuski, of the Insurance Bureau of Canada, put it this way:

> In a competitive economy — and I know that Parliament wants a competitive economy — it is absolutely essential that companies have access to information about the products and services that they in turn buy from other businesses, so that they can use this information to innovate and improve the products and service they sell their customers. Without access to work product information, innovation and competition will be stifled in the economy. (February 6, 2007)

There was a great deal of support from businesses for the approach taken by the British Columbia *Personal Information Protection Act*, which defines work product information as distinct from personal information under the Act. Section 1 of the B.C. law defines "work product information" as "information prepared or collected by an individual or group of individuals as a part of the individual's or group's responsibilities or activities related to the individual's or group's employment or business, but does not include personal information about an individual who did not prepare or collect the personal information." Most businesses support this definition because they believe it would provide certainty by allowing for consistent application.

In his brief to the Committee, the Information and Privacy Commissioner for British Columbia, David Loukidelis, noted that difficulties in interpretation and application can arise if a privacy law does not distinguish between personal information that is about someone as an individual and information they produce or compile as part of their work or business duties or activities. Interestingly, however, he had this to say when questioned by Committee members about the issue:

> As I mentioned, in British Columbia's law we have a definition of "work product information", and clearly the legislature, using specific language, has given me direction. It's my obligation, on a case-by-case basis, if the matter actually comes to me in a formal inquiry, to interpret and apply those words as intended by the legislature. Having said that, if we didn't have that definition, and if in fact we were to fall back on a definition of

> "personal information", which is "information about an identifiable individual", you would still have the same opening that has been taken here by my federal colleagues and in other provinces under their public sector legislation to try to interpret what information is "about" an individual in the sense intended by the legislature, and perhaps coming to the same result that has to be said. (November 29, 2006)

The issue of "work product" was of particular significance in relation to health information. IMS Canada, a principal provider of information, statistical research and analysis to the health sector, sought a definition of "work product" that is similar to the B.C. approach, but which also attempts to address some of the Privacy Commissioner's concerns that workplace monitoring and surveillance might inadvertently get caught up in a broad definition or interpretation of the term. Although the Privacy Commissioner had already found that physician prescribing patterns, information of particular concern to IMS, were not personal information for the purposes of PIPEDA, IMS would like this decision codified for greater certainty. The specific wording proposed by IMS was as follows:

> "work product information" means information prepared, compiled or disclosed by an individual or group as part of the individual or group's responsibilities related to their profession, employment or business. It does not include:
>
> i) personal information about an identifiable individual who did not prepare, compile or disclose the information; or
>
> ii) information collected, used or disclosed for the purposes of workplace surveillance. (February 8, 2007, brief, p. 34)

In response to the specific issue of whether information on doctor's prescriptions constitutes work product under PIPEDA, the Canadian Medical Association (CMA) takes the position that this data, along with other practice information, is the personal information of the physician, and physicians have legitimate privacy concerns about the use of this information by third parties for commercial purposes. While the CMA recommended that PIPEDA be amended to include physician information as personal information, it also made reference to Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector,* which requires regulatory oversight and gives individuals the right to opt out of the collection, use and disclosure of professional information.

The Quebec approach is considered something of a compromise in that it treats work product information with respect to professionals as something in-between personal and non-personal information. The Act allows for the disclosure of personal information on professionals about their professional activities without individual consent; however, this disclosure can only take place with the authorization and subsequent supervision of the Quebec Commission (in consultation with the relevant regulatory body). As well, the individual professional must have the opportunity to refuse to allow his or her information to be used for the disclosed purpose, and he or she must be regularly notified of the

intended uses of the information. The authorized recipient of the information must also report annually to the Commission on the implementation of the authorization, and the Commission must publish a list of authorized persons in his annual report.[8]

The Federal Privacy Commissioner consistently maintained throughout our hearings that this was not an easy issue to address; in other words, there is no quick fix or one clear model to follow. She would prefer to maintain the current definition of personal information and deal with questions of work product on a case by case basis. The Commissioner also submitted that adopting her proposed employee code under PIPEDA[9] would resolve many of the issues associated with work product in a manner that would not threaten other workplace privacy rights.

This Committee recognizes that the issue of work product is not sector-specific. It is a matter that cuts across the full realm of commercial and employment activities. The Committee believes that there is need for clarification within PIPEDA as to what is work product as opposed to personal information under PIPEDA. While we are reticent to recommend specific wording in such a contentious area, we recommend that consideration be given to the B.C. definition, the definition proposed by IMS, as well as the approach taken by Quebec with respect to professional information.

Recommendation 2

The Committee recommends that PIPEDA be amended to include a definition of "work product" that is explicitly recognized as not constituting personal information for the purposes of the Act. In formulating this definition, reference should be made to the definition of "work product information" in the British Columbia *Personal Information Protection Act,* the definition proposed to this Committee by IMS Canada, and the approach taken to professional information in Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector.*

2. Destruction

Principle 5 of Schedule 1 of PIPEDA addresses the issue of retention of personal information. Essentially, personal information shall be retained by an organization only for so long as is necessary to fulfill the purpose for which it was collected. After the information has served its intended purposes, and been retained for any prescribed periods, it should be destroyed, erased or made anonymous in accordance with disposal policies maintained by the organization (Principle 4.5.3). Principle 7 of the Schedule imposes security

---

8 An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q. c. P-39.1, s. 21.1.

9 See Consent part of the report regarding employee/employer relationships.

safeguards on the destruction process, such that care must be used in the disposal or destruction of personal information to prevent unauthorized parties from gaining access to the information (Principle 4.7.5).

In its appearance before the Committee, the National Association for Information Destruction (NAID) proposed a number of recommendations to ensure safe information destruction, something the organization feels is not happening in enough cases. Indeed, Mr. Dave Carey of NAID provided the Committee with a number of examples in support of the need for information destruction requirements to be spelled out in legislation. He summed things up for the Committee in this way:

> On any given day, it would not take long to find personal information being discarded, intact and accessible to the public. Careless disposal in dumpsters or garbage bins is the obvious example. Keep in mind as well, however, that recycling alone is not safe information destruction. Documents may still remain intact and vulnerable to privacy breaches for extended periods of time before being recycled. Privacy protection is no longer simply a human rights issue. Violating the rights of others by casually discarding their personal information provides much of the feedstock for what has become a global epidemic of identity fraud. According to a study conducted in the United States, the vast majority of identity theft results from low-tech access to personal information such as dumpster diving. (February 8, 2007)

NAID therefore recommended that the following definition of "destruction" be added to PIPEDA:

> For the purposes of principle 4.5 of Schedule 1, destruction is defined as the physical obliteration of records in order to render them useless or ineffective and to ensure reconstruction of the information (or parts thereof) is not practical. Destroy is defined as the act of destruction. (NAID Canada, letter dated February 21, 2007)

In its submission to the Committee,[10] the Ontario Ministry of Government Services stressed the need for greater education for organizations in terms of the secure destruction of personal information. As a result of the prevalence of identity theft in this country, the Ministry recommended that the Privacy Commissioner enhance her guidance on this issue by providing greater specificity on the steps organizations should take to destroy paper records and electronic media to ensure personal information is permanently destroyed or erased in an irreversible manner.

The Committee agrees that the proper destruction of personal information is an integral component of any personal information protection regime. Indeed, the privacy safeguards built into PIPEDA could be undermined if there is no specific destruction requirement in the Act. We therefore recommend that a definition of "destruction" be added to PIPEDA that would provide guidance to organizations on how to properly

---

10 December 2006, p. 8.

destroy both paper records and electronic media. We have considered the definition of destruction, both in *The Concise Oxford Dictionary*, 10th ed., and *Le Petit Larousse illustré 2002*, and we commend these definitions for consideration in this regard.

Recommendation 3

The Committee recommends that a definition of "destruction" that would provide guidance to organizations on how to properly destroy both paper records and electronic media be added to PIPEDA.

CONSENT

1. General Principles

Consent is the cornerstone of most data protection statutes and is no less so in PIPEDA. With very limited exceptions, the Act requires knowledge and consent for the collection, use and disclosure of personal information in the course of commercial activities. The consent principles are set out in Principle 3 of the *CSA Model Code for the Protection of Personal Information*, which forms Schedule 1 of the Act. The difficulty with these general principles seems to be in reconciling them in a manner that reflects commercial realities and, at the same time, provides adequate privacy protection for consumers.

Consumer representatives and privacy advocates who appeared before us argued that it is extremely difficult to use the language of a voluntary consensus-driven document (the CSA Model Code)[11] as a basis for legislation. They argue that the wording of the consent principles is too vague and thus subject to wide-ranging interpretations which does little to help clarify what is actually required under the law. In its brief to the Committee, the Public Interest Advocacy Centre provided these comments:

> Schedule 1 of PIPEDA contains a broadly-worded "Consent Principle." This principle provides a general framework for thinking about consent for privacy purposes in a commercial context; however, its language provides very little in the way of concrete assistance to businesses and consumers looking for a definitive statement of what consent is, what consent is required under the Act and how to obtain it.
>
> For instance, the Model code instructs that when it comes to obtaining consent, "the form of consent sought by an organization may vary, depending upon the circumstances and the type of information." Similarly, the Code instructs that "in obtaining consent the reasonable expectations of the individual are also relevant" and that "the way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected." It is obvious that these consent provisions permit both the

[11] See footnote 4.

> organization and the individual to argue that any processes set-up to obtain consent are deficient, or sufficient, from the point of view of either the individual or the business. (October 23, 2006, p. 14)

Arguments were also raised that PIPEDA's vague consent provisions are contributing to a significant lack of compliance with the legislation. In a report released in April 2006[12], the Canadian Internet Policy and Public Interest Clinic (CIPPIC) surveyed 64 on-line retailers and found that most are not obtaining meaningful consent to secondary uses and disclosures of consumer information. CIPPIC felt that its findings not only indicated an incentive/compliance problem, but also a lack of understanding of the consent requirements under the Act. It therefore recommended that a definition of "consent" be added to the legislation or at least clear preconditions and criteria for each of the three forms of consent (express, implied, deemed/opt-out). Reference was made to both the Alberta and British Columbia private sector data protection laws, which set out requirements for valid consent. The Ontario Ministry of Government Services, in a submission dated December 2006, also supported the idea that PIPEDA be amended to define and distinguish between different forms of consent in order to clarify both the obligations of organizations and the privacy rights of consumers.

Organizations generally support the consent principles as set out in PIPEDA because they provide the flexibility necessary for operating a business. It is also felt that the Act allows both businesses and consumers the ability to judge when additional information is required in order to make consent meaningful, and as such, there is no need to amend PIPEDA in this respect. In its brief to the Committee, the Canadian Marketing Association (CMA) had this to say on the definition of consent under PIPEDA:

> There are three forms of consent, which are currently recognized in the marketplace and are fundamental to information-based marketing activities. These forms of consent are the internationally recognized standard of industry and are specifically outlined in the CSA Model Code and in Chapter 5 of the Statutes of Canada 2000. They are: positive or express (opt-in) consent when dealing with sensitive information; negative option (opt-out) consent for the use of information for marketing purposes or for the transfer of non-sensitive information to third parties; and, implied consent, which allows a business to communicate with its existing customers. As outlined earlier in this brief, for many years CMA members have had to follow these forms of consent in their interactions with consumers. These were also the forms of consent that were recognized in PIPEDA, its related regulations and the interpretative findings of the Privacy Commissioner. The CMA feels strongly that these current definitions and applications of the three forms of consent should not be altered. (December 4, 2006, p. 11)

---

12 *Compliance with Canadian Data Protection Laws: Are retailers measuring up?* at http://www.cippic.ca/en/bulletin/compliance_report_06-07-06_(color)_(cover-english).pdf.

Although the Privacy Commissioner did not specifically address the issue of consent in her appearances before the Committee, she has issued a fact sheet on determining the appropriate form of consent under PIPEDA.[13] The document is intended to provide guidance to organizations by identifying the consent principles under the Act and providing illustrations of how they have been interpreted and applied by the Office of the Privacy Commissioner.

While the Committee appreciates the concerns raised by consumer and privacy advocates about the vagueness of the consent principles found in Schedule 1 of PIPEDA (the CSA Model Code), we are averse to making any changes to the CSA Model Code portion of the Act given the enormous amount of consultation that went into crafting this standard, and the complexity of the compromises reached. That being said, we feel it is important that people have a clear understanding of the form and adequacy of consent required by PIPEDA. This is better set out in legislation than left to the Commissioner's guidelines or court decisions. We therefore recommend that consideration be given to clarifying in the legislation what is required for consent under PIPEDA and distinguishing between express, implied and deemed/opt-out consent. Reference should be made in this regard to the Alberta and British Columbia *Personal Information Protection Acts*.

Recommendation 4

The Committee recommends that PIPEDA be amended to clarify the form and adequacy of consent required by it, distinguishing between express, implied and deemed/opt-out consent. Reference should be made in this regard to the Alberta and British Columbia *Personal Information Protection Acts.*

2. Exceptions

A. Employee/Employer Relationship

As noted at the beginning of this report, PIPEDA is a law that establishes rules governing the collection, use and disclosure of personal information in the private sector, but only in the course of commercial activities. The Act also seeks to regulate employee information, but due to jurisdictional issues, only in relation to federally regulated employment. The issue brought before this Committee was whether a consent model designed for commercial contexts can be applied to the employment milieu.

---

[13] http://www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp.

FETCO (Federally Regulated Employers — Transportation and Communication) argued strenuously that the current consent model under PIPEDA does not lend itself to the workplace environment. A number of employment issues were raised by FETCO, some of which we have addressed elsewhere in the report (i.e. work product and business contact information). FETCO's principal concern, however, relates to consent. It is FETCO's position that a definition of "personal employee information" should be added to PIPEDA, and that employee consent should not be required for the reasonable business use, collection or disclosure of any information related to managing the employment relationship. FETCO put forth the following options in its brief to the Committee:

> Different options exist for dealing with employee consent including reliance on implied or deemed consent, or even eliminating the requirement for employee consent for the collection, use or disclosure of personal information related to managing reasonable aspects of the employment relationship (similar to the approaches used in BC and Alberta). It is recommended that issues surrounding employee consent be reconsidered and addressed during the review process (December 2006, p. 4).

Once again, reference is made to the British Columbia and Alberta *Personal Information Protection Acts* which tackle the employment issue from another angle. The Information and Privacy Commissioner for British Columbia, David Loukidelis, outlined for the Committee the approach taken in his province:

> It is not necessary for an organization in British Columbia to get employee consent to collect, use, or disclose what is called employee personal information. This is not to say that employers have free rein, however, when it comes to collecting or using their employee's personal information, because the definition of "employee personal information" stipulates very clearly that it is only the information that an employer collects solely for purposes reasonably required to establish, manage, or terminate an employment relationship with that particular individual. The legislation also imposes a requirement that any collection, or use, or disclosure of that kind of information must be for purposes reasonably related to the actual work relationship. Instead of focusing on consent, recognizing that consent in the employment context is often coerced or that employees are under pressure to agree to employer practices, recognizing that it's not appropriate, for example, to ask an employer to get the consent of an employee who's suspected of defrauding the company to being put under surveillance — you're hardly going to get the suspect who's allegedly stealing from you to consent to that — instead of having to go through the consent route, it has been decided that you should be able to collect, use, or disclose personal information so long as it fits within the definition (November 29, 2006)

At the start of our hearings, the Privacy Commissioner cautioned about adopting the Alberta and B.C. approaches to employee information. Although acknowledging that personal information about employees has been a source of some of her most challenging complaints under PIPEDA, the Commissioner expressed concern that exempting large portions of employees' personal information from the consent process would take away rights that they currently have under PIPEDA. At the end of this review process, however, the Commissioner presented us with what she believes is a means by which all concerns might be addressed. She recommended that consideration be given to adopting the Alberta model, a reasonable purposes-based employee code, that also incorporates

Quebec's approach to protecting employee personal information. Thus any exemption for employee information must be accompanied by a requirement to consider employee dignity and an assessment of whether there would be an undue intrusion into an employee's personal life.

The Commissioner stressed that setting the specifics of her proposed regime would not be easy; however, she suggested that the use of section 7 of the Act, exemptions for collection, use and disclosure without consent, could contain a provision that would permit such exemptions for the purposes of establishing, managing or terminating an employment relationship. In her opinion, incorporating the concept of dignity would also enhance the Commissioner's ability to examine the full content of a complaint, in order to ensure that an employee consent exemption is not stretched too far. In this regard, she provided an example of a consent exemption stretched to incorporate such privacy intrusions as workplace surveillance.

The Committee agrees that the consent principle in PIPEDA does not fit easily into the workplace setting; however, we are mindful that creating exceptions to the consent requirement for employee/employer relationships or creating a separate employment code, is a complex undertaking. We therefore recommend that the government look to the models that currently exist in Quebec, British Columbia and Alberta in order to craft a suitable federal approach that ensures both a workable model for the functioning of employment relationships and the protection of the privacy rights of individual employees.

Recommendation 5

The Committee recommends that the Quebec, Alberta and British Columbia private sector data protection legislation be considered for the purposes of developing and incorporating into PIPEDA an amendment to address the unique context experienced by federally regulated employers and employees.

B. Investigative Bodies

PIPEDA contains two provisions that allow for the disclosure of personal information without the knowledge or consent of the individual to an investigative body. Section 7(3)(d) provides for such disclosure to be made on the initiative of an organization to an investigative body for certain purposes, and section 7(3)(h.2) permits an investigative body to release information for purposes related to the investigation of a breach of an agreement or contravention of the laws of Canada or a province. Investigative bodies are specified by regulation, and there are currently about 75 investigative bodies so designated.

Most business organizations that we heard from felt that PIPEDA should be amended to deal with problems experienced in terms of the nature and operation of investigative bodies and the designation process. In particular, it was argued that there are

many inconsistencies between the section 7 exemptions for collection, use and disclosure that frustrate the efforts of organizations in detecting and preventing fraud. The Canadian Bankers Association had this to say in its brief to the Committee:

> There are inconsistencies between the exemptions for collection, use and disclosure in the Act that can make it difficult for the banks to prevent fraud against their customers, other customers and the bank. In their efforts to prevent and investigate fraud against their customers and the banks themselves, banks frequently encounter situations where they need to be able to collect, use and disclose personal information without consent but are unable to do so due to the Act's inconsistencies among section 7(1), 7(2) and 7(3). For instance, while the Act allows an organization to collect and disclose information relating to a breach of an agreement, it does not allow for internal use of that same information in the course of the investigation to prevent further fraud against that customer, other customers or the bank. (January 2007, p. 3)

To remedy these concerns, it was suggested by some witnesses that instead of designating investigative bodies through regulation, a definition of "investigative bodies" could be added to the Act whereby bodies could self-designate according to a list of criteria. On the other hand, many organizations argued in favour of doing away completely with the "investigative body" approach under PIPEDA. They recommended that the Committee amend PIPEDA to follow the approaches taken by Alberta and British Columbia, which define the term "investigation" and allow collection, use and disclosure without consent for that purpose. The B.C. Act specifically includes fraud prevention in its definition.

The Privacy Commissioner believes that the current approach to designating investigative bodies, though cumbersome, is working adequately and does not need to be altered at this time. In her background document prepared for the Committee, the Commissioner noted that support for the current designation process is based on the transparency and oversight that stems from the regulatory process particularly as privacy impact assessments must be submitted as part of the application process. As well, the regulatory process ensures that there is a clear public listing of organizations designated as investigative bodies under the Act.[14]

The Committee supports the idea of an investigation exception to the consent principles under PIPEDA. We are concerned about the lack of consistency in section 7 of PIPEDA in this respect and in the interests of harmonization, we recommend that the approach taken by the Alberta and British Columbia private sector legislation be followed. These two second generation Acts allow for the collection, use and disclosure of personal

---

14 Office of the Privacy Commissioner of Canada, Statutory Review of the PIPEDA: Background Information on the OPC's Consultation, November 27, 2006, p. 12.

information without consent for the purposes of an investigation, which is defined to include an investigation of a breach of an agreement, a contravention of a federal or provincial law or circumstances or conduct that may result in a remedy available at law.

Recommendation 6

The Committee recommends that PIPEDA be amended to replace the "investigative bodies" designation process with a definition of "investigation" similar to that found in the Alberta and British Columbia *Personal Information Protection Acts* thereby allowing for the collection, use and disclosure of personal information without consent for that purpose.

C. Business Transactions

Numerous witnesses representing business interests spoke to the Committee about the lack of a provision in PIPEDA that would allow an organization to disclose personal information to prospective purchasers or business partners without the consent of the individual affected. Businesses often need to share information (such as client lists) to evaluate whether to proceed with a transaction — perhaps a merger, acquisition or sale of business — without the cumbersome necessity of obtaining every customer's consent.

The Privacy Commissioner's PIPEDA Review Discussion Document[15] indicates that several provincial data protection laws, such as Ontario's *Personal Health Information Protection Act* (PHIPA) and the Alberta and British Columbia *Personal Information Protection Acts* (PIPAs), allow disclosures without the individual's consent for business transaction purposes, subject to stringent confidentiality agreements. A number of witnesses before this Committee argued that it would be appropriate to include a similar provision in PIPEDA, along the lines of the Alberta or British Columbia models, to facilitate commercial transactions and to protect commercial secrets in a competitive business environment.

Section 22 of Alberta's *Personal Information Protection Act* sets out a regime for the disclosure of personal information without consent in the course of a business transaction, which is defined broadly to mean a transaction consisting of, for example, the purchase, sale, lease, merger or amalgamation or any other type of acquisition or disposal of an organization. Organizations are permitted to share personal information if necessary to determine whether to proceed with the transaction, and then to carry out the transaction. Obligations are set out for the return or destruction of the information if the transaction does not go ahead.

---

15 Ibid. p. 19.

Section 20 of the British Columbia *Personal Information Protection Act* permits similar information sharing, adding a requirement that the disclosed information be used only for the purpose for which it was collected, and that those whose personal information is disclosed are informed about the disclosure and the business transaction that has taken place.

The Canadian Medical Association asked that any new provision pertaining to the sale or transfer of a business explicitly recognize the unique situation of physicians and patient information. The Association had this to say:

> Physicians are striving to deliver timely quality care to patients, often with competing and multiple demands. Physicians are therefore seeking assurances from lawmakers that any amendments to PIPEDA will take into account the potential impact on them and their patients. Therefore, we seek assurances that, one, health care is recognized as unique when it comes to the disclosure of personal information before the transfer of a business, such as one physician transferring his or her practice to another. This is already regulated at the provincial level through the appropriate licensing bodies. As a general rule, physicians must give notice to the public, whether via a newspaper ad or a notice in the office, about the change in practice. (December 13, 2006)

The Privacy Commissioner, in her final submission to the Committee, advocated an amendment to PIPEDA that would create an enhanced version of the Alberta merger or sale of business model. In terms of enhancements, the Commissioner recommends a due diligence requirement that would limit information sharing to the least amount of personally identifiable information possible. As well, after a transfer of ownership, all individuals whose information has been transferred without consent should be notified about the transfer as soon as possible. Finally, the new owner should be required to adhere to the selling organization's policies respecting privacy until all individuals have had an opportunity to choose whether they want to have a relationship with the new owner.

This Committee agrees that PIPEDA must be amended to create an exception to the consent requirement in cases of business transactions or corporate restructuring. Indeed, we note that none of our witnesses opposed such an amendment. The question, however, is what is the best approach to facilitating these transactions while at the same time protecting, to the greatest extent possible, the privacy interests in the personal information that is shared. We note that a number of our witnesses, including the Privacy Commissioner, supported the Alberta model in particular, and we therefore recommend the adoption of this approach along with the enhancements to it that were proposed by the Commissioner.

Recommendation 7

The Committee recommends that PIPEDA be amended to include a provision permitting organizations to collect, use and disclose personal information without consent, for the purposes of a business transaction. This amendment should be modeled on the Alberta *Personal Information Protection Act* in conjunction with enhancements recommended by the Privacy Commissioner of Canada.

D. Principal-Agent Relationship

The Insurance Bureau of Canada (IBC) brought a principal-agent issue to the attention of the Committee. IBC is concerned about the lack of a provision that clarifies this relationship in PIPEDA. For example, it was pointed out that in a principal-agent relationship, the consent that is granted by the principal should be able to be relied upon by the agent in carrying out certain functions. In the insurance industry, investigations and claims settlements may be outsourced to independent adjusting companies, and IBC seems concerned that this outsourcing could be considered disclosures for the purposes of the Act and as such, would require a separate consent for the agent. In its brief to the Committee, IBC had this to say:

> Outsourcing of business functions to agents is a necessary and integral part of business practices for all business sectors. A reasonable person, who is referred to sections 3 and 5(3) of PIPEDA, would expect that an insurer, like any other business, would outsource certain functions to others who act as agents on behalf of the insurer. If the agent wants to use the personal information for its own purpose, then the agent would have to obtain a separate consent from the individual for that separate purpose. (November 24, 2006, p. 12)

IBC referred to section 12(2) of the British Columbia *Personal Information Protection Act* as a possible solution to the problem it identified. In the alternative, it suggested that definitions of "agent," "use" and "disclose" could be added to PIPEDA. Section 12(2) of the B.C. Act provides:

> An organization may collect personal information from or on behalf of another organization without consent of the individual to whom the information relates, if
>
> (a) the individual previously consented to the collection of the personal information by the other organization, and

(b) the personal information is disclosed to or collected by the organization solely

(i) for the purposes for which the information was previously collected, and

(ii) to assist that organization to carry out work on behalf of the other organization

The Canadian Bar Association, in its submission to the government in preparation for this review,[16] also raised the need to clarify the existence of an agent concept in PIPEDA. The Association pointed out that the third party processing rule in Principle 4.1.3 of Schedule 1 of the Act, which requires organizations to use contractual or other means to ensure a comparable level of protection while the information is being processed by a third party, does not explicitly state whether such processing is considered a transfer or a disclosure, the latter of which would require consent. As well, the Association felt that the Act is unclear about whether the processing exception is to be strictly limited to transfers of information for payroll, pensions and other such administrative purposes (i.e. as opposed, for example, to work conducted by a private investigator retained by the organization). The Association therefore suggested that PIPEDA be amended to confirm that an organization may collect, use and disclose personal information from or on behalf of a principal organization without the consent of the individual to whom the individual relates, but only if the individual previously consented to the collection, use and disclosure of the information by the principal organization, and the information is collected, used and disclosed to assist in carrying out work on behalf of the principal organization.

The Committee agrees that any confusion about the existence of a principal-agent relationship in PIPEDA should be cleared up. Given that the recommendation of the Canadian Bar Association appears to be essentially the same as section 12(2) of the B.C. Act, we recommend that PIPEDA be amended to clarify the principal-agent relationship under PIPEDA with reference to the B.C. legislation.

Recommendation 8

The Committee recommends that an amendment to PIPEDA be considered to address the issue of principal-agent relationships. Reference to section 12(2) of the British Columbia *Personal Information Protection Act* should be made with respect to such an amendment.

16 Canadian Bar Association, National Privacy and Access Law Section, Preparing for the 2006 Review of the *Personal Information Protection and Electronic Documents Act*, August 2005, pp. 21-24.

E. Litigation Process/Legal Proceedings

Related to concerns expressed by witnesses about the way in which PIPEDA applies to law enforcement/investigations (see Investigative Bodies, above), the Committee heard testimony that PIPEDA should also be rendered neutral with respect to the litigation process. Brian Bowman of the Canadian Bar Association had this to say in his submission to the Committee:

> In other words, it [PIPEDA] should not affect pre-existing and commonly held litigation processes that have evolved for decades and hundreds of years. PIPEDA contains a number of specific exemptions to the consent requirement that require amendment. The current exceptions relating to litigation are too narrow and should, at a minimum, be broadened to ensure that well-established litigation procedures are not impeded. This narrowness is evident in the investigation exceptions, the one-way disclosure, the collection and use of debt disclosure information, and the limitation on disclosure throughout the litigation process. The result is inadequate coverage of all aspects of the process: pleadings, oral discovery, mediation, private arbitration, settlements, solicitor communications, and other non-court ordered exchanges of information. There should be a broad exclusion for information legally available to a party to a proceeding that would override specific exceptions currently found in PIPEDA. (December 11, 2006)

The Canadian Bar Association recommended that the models for litigation provided in the British Columbia and Alberta *Personal Information Protection Acts* be considered in relation to PIPEDA. Sections 12, 15 and 18 of the British Columbia Act permit the collection, use and disclosure of personal information without consent where it is reasonable to expect that the collection, use or disclosure with consent would compromise the availability or accuracy of the personal information, and the collection, use or disclosure is reasonable for an investigation or proceeding. Sections 14, 17 and 20 of the Alberta Act permit the collection, use and disclosure of personal information without consent where the collection, use or disclosure is reasonable for the purposes of an investigation or a legal proceeding. Both Acts define "proceeding" and "legal proceeding" as a civil, criminal or administrative proceeding that is related to a breach of an agreement, a contravention of a federal or provincial Act or a remedy available at law or under common law or in equity.

In a somewhat similar line of argument, the Insurance Bureau of Canada (IBC) sought an exemption to the consent requirement in PIPEDA in relation to witness statements. IBC recommended that the definition of "personal information" be modified to clarify that personal information expressed by one individual (the witness) about another (the subject) is the personal information of the witness. It also felt that section 7 of PIPEDA, exemptions to the consent requirement, should be amended to provide that an organization may, during the course of investigating and settling contractual issues or claims for loss or damages, collect, use and disclose a witness statement without the subject's knowledge or consent. The following rationale was provided for IBC's proposals:

> In our view, it would be unreasonable to prevent the insurer — and the court and jury, if a lawsuit is commenced and the matter proceeds to trial — from collecting all of the relevant facts related to the incident. We are opposed to the view that an insurer should obtain the consent of the claimant or potential claimant before obtaining witness

> statements. This would have serious consequences as it would effectively allow one individual to prevent another individual (witness) from reporting what they saw or heard and would prevent an insurer, and by extension the court, from collecting all of the relevant facts about the incident. (November 24, 2006, brief, p. 4)

The Committee agrees that there appear to be some inconsistencies in the current exceptions to the consent provisions of PIPEDA which could be better dealt with in a broader approach. We heard testimony about this in a number of areas. Specifically, with respect to litigation or legal proceedings, the Committee believes that PIPEDA's privacy protection provisions should not impede the proper conduct of litigation, and that a broad amendment may be required to exempt from the consent requirement information necessary for legal proceedings. This should be done in a manner that would bring PIPEDA into alignment with the British Columbia and Alberta statutes.

The Committee is also concerned about the testimony it received with respect to witness statements and the issue of whose personal information is contained therein. We appreciate that insurance companies are struggling, in the course of investigating and settling insurance claims, with issues of whether, in order to obtain a witness statement, they must seek the consent of the claimant or potential claimant because his or her personal information is contained therein. As well, we received testimony that insurers are reluctant to provide access to witness statements to claimants who assert that they are entitled to these documents on the basis that it is their personal information.

While we have not heard evidence in this regard from organizations representing privacy interests, including the Federal Privacy Commissioner, we feel that consideration should be given to whether there might be ways in which the issue of witness statements could be addressed in PIPEDA other than by means of our proposed investigation exception (Recommendation 6) and the following litigation/legal proceedings exception.

Recommendation 9

The Committee recommends that PIPEDA be amended to create an exception to the consent requirement for information legally available to a party to a legal proceeding, in a manner similar to the provisions of the Alberta and British Columbia *Personal Information Protection Acts*.

Recommendation 10

The Committee recommends that the government consult with the Privacy Commissioner of Canada with respect to determining whether there is a need for further amendments to PIPEDA to address the issue of witness statements and the rights of persons whose personal information is contained therein.

F. Individual, Family and Public Interest Exceptions

Section 7(3)(e) of PIPEDA allows for a disclosure of personal information without consent "to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure." Some witnesses, however, felt that this provision was not broad enough to cover other situations that would equally warrant such an exemption.

The Committee heard from the Insurance Bureau of Canada (IBC) and the Financial Advisors Association of Canada (Advocis) that it would be helpful to have an exemption to PIPEDA's consent requirements with respect to beneficiaries (e.g. under a will or insurance policy). IBC, for example, referred to instances within the insurance industry where a policy is applied for and issued in the name of one individual, but other individuals are named or listed as additional insureds or beneficiaries. IBC therefore asked for a provision within PIPEDA that would allow an individual to give consent on behalf of another individual when the other individual can claim the benefit of a product or service for which their personal information was provided. Reference was made to section 8(2) of the B.C. *Personal Information Protection Act* which provides that:

> 8(2) An individual is deemed to consent to the collection, use or disclosure of personal information for the purpose of his or her enrollment or coverage under an insurance, pension, benefit or similar plan, policy or contract if he or she
>
> (a) is a beneficiary or has an interest as an insured under the plan, policy or contract, and
>
> (b) is not the applicant for the plan, policy or contract.

Advocis recommended that consideration be given to section 14(a) of Alberta's *Personal Information Protection Act* for the purposes of allowing financial advisors to collect information about third parties in the course of developing a financial plan for clients. Section 14(a) allows an organization to collect personal information without consent where "a reasonable person would consider that the collection of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent."

The Canadian Bankers Association (CBA) raised the issues of natural disasters where family members want to determine whether a loved one has survived and are seeking information about them, and employment situations where an employer cannot reach an employee and therefore needs to convey important information to a next of kin or designated contact. The banks were also concerned about the incidence of elder financial abuse and the inability of PIPEDA to address this problem. Mr. Warren Law of the CBA outlined the banks' concern:

> An example of such a situation in the banking context is where a banker suspects financial abuse, particularly with seniors, and when a customer is withdrawing money from his or her account and it appears that the customer may be under pressure from the person accompanying him or her, or the withdrawal is uncharacteristic of that person.
>
> Prior to PIPEDA, under common law, banks were able to disclose their suspicions about abuse to the authorities, to the vulnerable customer's family, or to another responsible person who might be able to investigate and stop any abuse. Financial abuse of the elderly is a significant issue in Canada. The public and families of such customers expect bankers to help prevent any abuse. Under the current legislation, though, while branch employees want to help, they are not allowed to because there are no exceptions that cover such situations. We are recommending an exemption for disclosure without consent when it is in the public interest. (January 30, 2007)

The CBA recommends that section 7(3) of PIPEDA be amended to permit disclosure of personal information to appropriate authorities, next of kin or a designated contact for the individual when the release of that information is in the individual's or the public's interest.

In its submission to Industry Canada in anticipation of this Committee's review,[17] the Canadian Bar Association recommended that certain factors should be taken into consideration when assessing the reasonableness of relying on consent obtained indirectly from an individual through another person. For example, the nature of the transaction, the sensitivity of the personal information, the nature of the relationship between the individual and the person confirming his or her consent and whether the collection, use or disclosure benefits the individual are all factors that should be set out in the legislation as assessment criteria.

It is the Privacy Commissioner's position that there may well be some very limited exceptions in this area that should be considered for the purposes of a consent exemption. Examples cited by the Commissioner included disclosures to the family of an injured, ill or deceased individual and notification in the case of an emergency in a community setting.

As noted at the beginning of this report, the Committee generally recognizes the need to harmonize PIPEDA with provincial private sector data protection laws. This is an instance where there is a need to consider the relevant provisions found in Quebec, Alberta and B.C. The Committee is cautious, however, about recommending the use of the term "public interest" in this context given its potential vagueness and the fact that we have heard a lot of testimony around the vagueness of terms or the lack of clarity in PIPEDA's current provisions. On the other hand, we are mindful that a broad term like "public interest" may be necessary to provide sufficient flexibility to such an exemption.

---

17 Ibid., pp. 42-43.

Recommendation 11

The Committee recommends that PIPEDA be amended to add other individual, family or public interest exemptions in order to harmonize its approach with that taken by the Quebec, Alberta and British Columbia private sector data protection Acts.

G. Law Enforcement/National Security Interests

i. Section 7(3)(c.1)

Section 7(3)(c.1) of PIPEDA allows organizations to disclose personal information to government institutions without the knowledge or consent of the individual and without judicial authorization in certain specified circumstances related to law enforcement and national security. A number of witnesses raised concerns about what is meant by "government institution" in this provision and suggested that the term be clarified because disclosures to such bodies are made without the knowledge or consent of the individual.

The Canadian Bar Association, for example, recommended that PIPEDA include a definition of "government institution" to specify whether disclosure is intended to encompass municipal, provincial, territorial, federal and non-Canadian entities. The Canadian Internet Policy and Public Interest Clinic (CPPIC) felt strongly that in view of Canadians' concerns about outsourcing of information processing and the powers of foreign agencies to access such data from private businesses, the phrase "government institutions" in sections 7(3)(c.1) and (d) of PIPEDA should be limited to Canadian government institutions. This would force foreign governments' requests for data about Canadians to be routed through Canadian government entities.

Another issue raised with respect to section 7(3)(c.1) had to do with the meaning of "lawful authority." Some witnesses, such as the BC Freedom of Information and Privacy Association and BC Civil Liberties Association were of the opinion that private companies should insist on seeing a court order from a law enforcement or investigative agency (except in exceptional and urgent cases) before disclosing any personal information pursuant to this section. On the other hand, we heard from the Canadian Association of Chiefs of Police (CACP), the Canadian Resource Centre for Victims of Crime and the RCMP that law enforcement efforts are actually being thwarted by stringent interpretations of PIPEDA with respect to obtaining non-sensitive personal information on a voluntary basis from companies. Mr. Clayton Pecknold of the Canadian Association of Chiefs of Police explained the problem to the Committee in this way:

> In another example, a police officer may be in the early stages of a missing person investigation, in which he or she is trying to determine if in fact a crime has occurred. Perhaps we may have to solicit the assistance of a financial institution because we need to know if that person bought gas at a particular gas station or if the person used a credit

card, or perhaps we need to find out if a person has a cell phone registered to him with a particular company. For this information we rely on paragraph 7(3)(c.1), which permits disclosure upon lawful authority, as my friend has already noticed. However, we are increasingly seeing some companies interpreting lawful authority to mean that a warrant or court order is required before they comply. This is an interpretation that is not, in our respectful view, consistent with the intent of the drafting of the act. Such an interpretation by companies, while no doubt grounded in a legitimate desire to protect their customers' privacy, is overly restrictive and defeats, in our view, the intent of paragraph 7(3)(c.1).(February 13, 2007)

The CACP, the Canadian Resource Centre for Victims of Crime and the RCMP all recommended that section 7(3)(c.1) be amended to make it clear that lawful authority does not mean that a warrant is required in order for there to be a disclosure.

The Committee agrees that there is a valid concern around what constitutes lawful authority for the purposes of disclosure under section 7(3)(c.1). Clearly something other than judicial authorization is required for the purposes of this section given that section 7(3)(c) provides for disclosure without knowledge or consent in compliance with a warrant or subpoena. We think it is important, for both organizations and law enforcement agencies, that what is meant by "lawful authority" be clarified in section 7(3)(c.1). Moreover, the Committee feels that consideration should be given to changing the word "may" in the opening part of section 7(3) in order to make the provision mandatory as opposed to permissive. We appreciate that, in light of the permissive nature of section 7(3) and its fit within the general framework of the Act, this might require restricting a mandatory approach to those disclosure provisions dealing with issues of law enforcement and national security.

The Committee also agrees that there is a need to clarify what is meant by the term "government institution" in sections 7(3)(c.1) and (d) of PIPEDA. Specifically, organizations should know whether the term is intended to encompass municipal, provincial, territorial, federal and non-Canadian entities.

Recommendation 12

The Committee recommends that consideration be given to clarifying what is meant by "lawful authority" in section 7(3)(c.1) of PIPEDA and that the opening paragraph of section 7(3) be amended to read as follows: "For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization shall disclose personal information without the knowledge or consent of the individual but only if the disclosure is [...]"

Recommendation 13

The Committee recommends that the term "government institution" in sections 7(3)(c.1) and (d) be clarified in PIPEDA to specify whether it is intended to encompass municipal, provincial, territorial, federal and non-Canadian entities.

ii. Section 7(1)(e)

Section 7(1)(e) was added to PIPEDA pursuant to the *Public Safety Act, 2002,* which in 2004 amended a number of federal laws in response to the events of September 11, 2001 in the United States. Prior to 2004, organizations subject to PIPEDA already had the ability to *disclose* personal information without the individual's knowledge or consent for reasons of national security, the defence of Canada, the conduct of international affairs or where required by law (sections 7(3)(c.1), 7(3)(d)(ii) and 7(3)(i)). The amendments brought about by the *Public Safety Act* added the ability of organizations to *collect* and *use* personal information without knowledge or consent of the individual for the purposes of making such disclosures. It is the new collection power that is most troubling to privacy advocates.

The Committee heard from some individuals as well as privacy rights organizations who argued that section 7(1)(e) of PIPEDA not only fails to fit into the balanced consent regime under the Act, but it also blurs the line between the private sector and law enforcement.[18] Murray Long, a privacy consultant, had this to say about the section:

> To understand the impacts of this change, it is important to consider the meaning of the word "collect". Whereas "use" relates to the management and various uses of existing personal information that has previously been collected, "collect" refers to the acquiring of new information that did not previously exist within the organization.
>
> Under the *Public Safety Act* amendment, organizations can now collect new information about their customers or employees or any other party where they believe there is a national security interest and for the purpose of eventually disclosing it to a security agency.
>
> This invites tremendous abuse of individual privacy rights. (February 6, 2007, brief, p. 8)

The Privacy Commissioner, in her submission to the Committee, raised serious concerns about the broad wording of section 7(1)(e). In her view, because the provision applies to any organization subject to PIPEDA, it has the undesirable effect of deputizing

---

[18] Professor Colin Bennett, Submission to a House of Commons Standing Committee on Access to Information, Privacy and Ethics, November 22, 2006, p. 12.

the private sector to carry out law enforcement activities without the corresponding public accountability.[19] As she did at the time of the passage of the *Public Safety Act, 2002,* the Commissioner continues to call for the removal of section 7(1)(e) from PIPEDA, or that it at least be made more restrictive.

In a letter dated March 20, 2007, that was hand delivered by the Chairman on that same day, the Committee asked the Minister of Public Safety for his assistance in addressing the issues raised by our witnesses on this matter. Specifically, the Minister was asked to appear or provide written comments within a week or so in order that the Committee could be timely in its reporting to the House of Commons. In the absence of any such response from the Minister, based on the testimony it received, and after considered debate by Committee Members, the Committee makes the following recommendation.

Recommendation 14

The Committee recommends the removal of section 7(1)(e) from PIPEDA.

PERSONAL INFORMATION OF MINORS

Some witnesses advocated including in PIPEDA special rules designed to protect children from improper collection, use or disclosure of their personal information. Professor Valerie Steeves, of the University of Ottawa, impressed upon the Committee the subtle ways in which children's personal information is collected when they are on the Internet. She described popular websites where, in order to be allowed to play the games available there, children must first fill out marketing surveys.

> These kids are nine and they are playing. They are not disclosing information for commercial purposes. Yet the kind of legislation that we have in place lets companies set up these kinds of environments and, through a very weak consent mechanism, capture that information and reconfigure it as a commercial commodity. (November 29, 2006)

Philippa Lawson, of the Canadian Internet Policy and Public Interest Clinic (CIPPIC), urged the Committee to recommend amendments to PIPEDA to create "special limitations regarding the collection of information from children, whose credulity and ignorance can easily be exploited by commercial interests."[20] CIPPIC recommended that there be included in the Act specific rules limiting the collection, use and disclosure of

---

19 Footnote 14, p. 11.

20 December 6, 2006.

children's personal information, along with strict penalties for violating these provisions. Reference was made in this respect to the *Canadian Code of Practice for Consumer Protection in Electronic Commerce* by the Canadian Marketing Association.

Responding to a discussion about the collection of personal information from children, the Information and Privacy Commissioner for British Columbia, David Loukidelis, made the following comments, saying that while some legislative steps have been taken in the United States, the issue is still under consideration in Canada.

> On the question of surveying children, clearly that introduces some very sensitive issues around the ability of youth to understand what it is they're entering into when they give up some of this information, sufficiently so that in the U.S., Congress passed the Children's Online Privacy Protection Act of 1998. Again, it is early days for these laws in Canada. For my part, I would hope that in British Columbia, we can, only three years into our law, continue to work with industry to try to ensure that in the case of children and generally in relation to some of these technological challenges, those general principles are adhered to and that the legislation works well in its present form without radically altering the approach to some of these technologies. (November 29, 2006)

The Canadian Bar Association (CBA) included a short discussion of issues relating to consent by minors in the brief it prepared in anticipation of the 2006 PIPEDA Review.[21] The CBA argued that there is uncertainty about whether minors can consent to participate in on-line activities without parental consent. Clarification is called for, it contends, about when minors can give such consent, and consideration should be given to stipulating a minimum age below which consent may not be given without parental approval. The CBA recommended that PIPEDA be amended to provide that minors can consent to the collection, use and disclosure of their personal information if they understand the nature of giving consent and its consequences, and that below a certain age (for example, 13 years) such consent must be given by a parent or legal guardian.

While the Privacy Commissioner's background document, *Statutory Review of the PIPEDA: Background Information on the OPC's Consultation,*[22] mentions that the issue of the personal information of minors was brought forward in its consultations by a consumer advocacy group, the Commissioner herself did not take a position on whether the Act should be amended to deal with it. This may be because the establishment of a specific age at which children are competent to act independently is an area of provincial jurisdiction. Nonetheless, the Committee believes that the issue of consent with respect to the collection, use and disclosure of personal information of minors in a commercial context is of sufficient importance to merit further study, including input from the Privacy Commissioner and other stakeholders.

---

21 See footnote 16, pp. 43-44.

22 See footnote 14, p. 33.

Recommendation 15

The Committee recommends that the government examine the issue of consent by minors with respect to the collection, use and disclosure of their personal information in a commercial context with a view to amendments to PIPEDA in this regard.

DATA OUTSOURCING (TRANSBORDER FLOWS OF PERSONAL INFORMATION)

In today's high-tech, globalized business environment, more and more information is being outsourced for processing. Along with this growing practice, however, comes the question of the extent to which Canadian privacy protection at home travels with personal information that is transferred to non-Canadian organizations. Most businesses feel that PIPEDA currently offers adequate privacy protection in this respect. Reference is made to PIPEDA's Accountability Principle (Principle 1, Schedule 1) which states that each organization is responsible for the personal information in its care. Specifically, Principle 4.1.3. provides that this responsibility extends to information that has been transferred to a third party for processing. The Information Technology Association of Canada (ITAC), in its brief to the Committee, summed up the views of the business community this way:

> PIPEDA's accountability principle demands that businesses in Canada communicate their privacy practices to the public in a transparent manner. It also requires that those businesses enter into contractual agreements with their third-party providers in all jurisdictions to ensure a similar level of protection for personal information transferred outside Canada. In this respect, PIPEDA, together with the law of contract and agency, works to deal with practical business, legal and technological realities [...] Placing further restrictions on transborder flows of information under PIPEDA could reduce the competitiveness of Canadian businesses in the global market. (December 11, 2006, p. 4)

Other witnesses, however, sought greater privacy protection mechanisms for trans-border information-sharing by the private sector. Arguments were made for more specific rules directed at the protection of personal information transferred outside of Canada and reference was made to the Quebec *An Act Respecting the Protection of Personal Information in the Private Sector*[23] which obliges people communicating information about Quebec residents to persons outside the province to take all reasonable care to ensure that the information is not disclosed to third parties without consent, except as provided by legislation. In his submission to the Committee, Brian Bowman of the Canadian Bar Association made a number of suggestions for consideration in this area:

---

23 Section 17.

> PIPEDA should contain appropriate precautionary requirements to protect information when it is transferred across borders. We have previously considered a number of alternatives to achieve this objective, such as a requirement that organizations transferring information to foreign entities enter into written agreements that would ensure security and protection of information against unauthorized access or disclosure in accordance with Canadian privacy law [...] In its earlier submission, the CBA section also analyzed options for notification or consent requirement for information transferred across a border. Each of these options would involve some form of notice to be provided to or consent obtained from the individuals whose information would be transferred outside of Canada. Amending PIPEDA to implement either a notice or a consent requirement to cross-border transfer of information requires a very careful consideration of the potential advantages and disadvantages of the approach. (December 11, 2006)

The B.C. Freedom of Information and Privacy Association and BC Civil Liberties Association also reminded us of the situation that arose in British Columbia with respect to the outsourcing of medical records to the United States and concerns about the reach of the U.S. *Patriot Act.* That law was passed in the wake of the events of September 11, 2001 as a means of increasing the U.S. government's ability to conduct searches and to seize or compel the disclosure of records. The B.C. government ultimately amended its public sector privacy legislation to address the concerns about possible unauthorized disclosures of personal information to U.S. authorities. In his appearance before the Committee, the Information and Privacy Commissioner for British Columbia, David Loukidelis, spoke to the B.C. outsourcing issue and outlined what he sees as the distinction between public and private sector data protection legislation in relation to trans-border information flows:

> The legislature, three weeks before that report was actually delivered with that conclusion, chose to amend the Freedom of Information and Protection of Privacy Act to make it even clearer that foreign court orders, foreign judicial process, could not reach extraterritorially into Canada with that effect, and to impose certain other requirements on public bodies in British Columbia around the protection of personal information of citizens.
>
> No such amendments were made to the *Personal Information Protection Act*. And I have from the outset, as it happens, drawn a distinction between the public sector situation, where citizens are not in a position to consent or not to consent to the decision by government to outsource the delivery of public services involving their personal health information, and the situation in the private sector, where, certainly in principle and I think realistically in practice, individuals can vote with their feet. If they're not content with the personal information practices of a particular business, they can take their business elsewhere and make that consumer choice. I think that is a real and meaningful and substantial distinction that justifies the different treatment across the public sector and private sector divide. (November 29, 2006)

The Federal Privacy Commissioner also sees no need for amendments to the federal private sector data protection legislation to deal with data outsourcing. In her view, this matter is best addressed through the guidance of PIPEDA's Accountability Principle

along with existing Treasury Board guidelines on contracting out.[24] The Commissioner pointed out that she is also working on this issue at the international level. For example, she is chairing a Working Group of the Organization for Economic Co-operation and Development (OECD) Working Party on Information Security and Privacy to address the cross-border challenges of effectively enforcing privacy laws.

The Committee agrees with the Privacy Commissioner that there is no need to amend PIPEDA with respect to transborder flows of personal information. In our view, the Act already contains sufficient accountability and allows for the necessary flexibility for businesses to ensure that personal information is privacy protected when it crosses our borders. We do, however, encourage the Commissioner to continue to work with organizations, as well as the federal government, to ensure appropriate guidance in this respect.

Recommendation 16

The Committee recommends that no amendments be made to PIPEDA with respect to transborder flows of personal information.

PERSONAL HEALTH INFORMATION

Although PIPEDA came into force on January 1, 2001, as a result of Senate amendments to Bill C-6 (PIPEDA), the law did not apply to personal health information until January 1, 2002. In its December 1999 report, the Standing Senate Committee on Social Affairs, Science and Technology observed a considerable amount of uncertainty surrounding the application of the privacy protection provisions of Bill C-6 to personal health information.

The Senate Committee felt that this uncertainty required clarification and that further legislative action was desirable. In particular, it was felt that more specific provisions regarding, for example, issues of informed consent and the secondary use of personal health information should be developed. The Committee therefore recommended that the bill be amended to include a definition of "personal health information", and that the application of the law to personal health information be suspended for a period of one year following the coming into force of the bill. The Committee hoped that this temporary suspension of Part 1 of the bill would motivate stakeholders and governments to formulate an appropriate solution for the protection of personal health information.

---

24 "Privacy Matters: The Federal Strategy to Address concerns About the USA Patriot Act and Transborder Data Flows." Treasury Board of Canada Secretariat, http://www.tbs.sct.gc.ca/pubs_pol/gospubs/TBM_128/pm-prp/pm-prp_e.asp.

According to testimony that this Committee received during its review of PIPEDA, the delayed application of PIPEDA to personal health information allowed the federal government to work with the health care community, in conjunction with the Office of the Privacy Commissioner, on the development of a set of guidelines known as PIPEDA Awareness Raising Tools (PARTs). Dr. Wayne Halstrom, of the Canadian Dental Association (CDA), had this to say about the PARTs initiative:

> We at the CDA appreciated the federal government's initiative to produce information that would help our members understand their obligations under PIPEDA versus simply obtaining another legal opinion on how PIPEDA would apply to dentists. CDA was an integral member of the working group that met regularly with officials from the Privacy Commissioner's office, Justice Canada, Health Canada and Industry Canada to create the PIPEDA awareness-raising tools, as we've heard, the PARTs initiative for the health sector. This process created the final content for the federal government's interpretation of PIPEDA, a series of straightforward questions and answers that add clarity to the requirements around obtaining consent, disclosing personal health information to private insurance companies, office safeguards, and requests to change information on a dental record, to name but a few. (December 13, 2006)

While the CDA, the Canadian Medical Association and the Canadian Pharmacists Association all expressed support for the PARTs initiative, they also recommended that the PARTs document be given legal status or, in some way, referenced within PIPEDA. The Canadian Health Infoway Inc., in its brief to the Committee, also felt that this review would be an opportune time to clarify PIPEDA's application to the health care sector.[25]

The Committee appreciates the desire for clarity and consistency in terms of the application of PIPEDA to personal health information; however, we are not comfortable with adding yet another schedule to the Act, particularly when the PARTs document is essentially a question and answer sheet that is intended to assist in the understanding of PIPEDA and not serve as legal advice. The Committee therefore recommends that the government consult further with health care stakeholders, as well as the Office of the Privacy Commissioner in order to ascertain what, if anything, can be done to reference the elements set out in PARTs (e.g. with respect to implied consent) within the legislative framework of PIPEDA.

Recommendation 17

The Committee recommends that the government consult with members of the health care sector, as well as the Privacy Commissioner of Canada, to determine the extent to which elements contained in the PIPEDA Awareness Raising Tools document may be set out in legislative form.

---

25 February 2007.

POWERS OF THE FEDERAL PRIVACY COMMISSIONER

1. Order-making Powers

As noted at the beginning of this report,[26] PIPEDA is based on an ombudsman model in that the primary duty of the Privacy Commissioner is to investigate and make recommendations with respect to complaints from persons alleging that their privacy rights have been breached under the Act. The Supreme Court of Canada in *Lavigne* v. *Canada (Office of the Commissioner of Official Languages)*[27], describes the ombudsman role as follows:

> An ombudsman is not counsel for the complainant. His or her duty is to examine both sides of the dispute, assess the harm that has been done and recommend ways of remedying it. The ombudsman's preferred methods are discussion and settlement by mutual agreement.

Thus, while the Privacy Commissioner has investigative powers, the discretion to initiate complaints, the power to conduct an audit and publicly disclose information relating to the personal information management practices of an organization, she has no order-making powers under the Act.

A number of witnesses who appeared before us wanted PIPEDA amended to provide the Commissioner with order-making powers. It was argued that such powers would serve as a means of facilitating compliance with PIPEDA, cut costs and delays in the current process and generate a consistent body of case law that would allow both individuals and organizations to have a clearer understanding of their rights and responsibilities. Professor Colin Bennett, of the University of Victoria, expressed concern that the ombudsman model might not be the best fit with a private sector compliance law:

> The lesson I draw from this is that the ombudsman model, which is very good at mediating and resolving disputes between individuals and organizations, may not be very good when you're looking at a compliance model or regulatory model like this, where you're simply trying to get the organization concerned to comply with the law. Therefore, I think there's a mismatch between some of the goals of the law and the ombudsman model that is used to enforce it. (November 22, 2006)

Those favouring order-making powers for the Privacy Commissioner also referred to the three provinces with substantially similar private sector privacy legislation (Quebec, Alberta and British Columbia) wherein each privacy commissioner has the power to render binding decisions in certain cases. Referred to as "ombudsmen with a stick," these

---

26 Overview of the Act.

27 *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, at paragraph 39.

commissioners use their order powers sparingly; however, it is argued that the strong incentive these powers provide in facilitating reasonable settlements is essential to their overall effectiveness as commissioners.

In his appearance before the Committee, David Loukidelis, Information and Privacy Commissioner for British Columbia, had this to say about his order-making powers:

> Since the beginning of 2004, we've had an order-making power. However, it has to be emphasized that it is by no means the tool of first choice for our office, speaking for myself or indeed looking at the experience of our office [...] In the three years, just about, that PIPA has been in force, I've issued seven binding orders under PIPA. The remainder of the matters we have been able to deal with in a mediation type of approach, which is consistent with the approach taken, as I understand it, in every important respect, here in Ottawa by my federal colleague and in other commissioners' offices across the country. (November 29, 2006)

Most businesses and organizations who spoke to this issue preferred to maintain the existing ombudsman model because it provides a flexible, informal, accessible and cost-effective dispute resolution process with formal and binding review still available via the courts. Put another way, they feel that the current model effectively balances the rights of individuals to the protection of their personal information and the rights of organizations to use that information in legitimate ways for their commercial purposes. Organizations prefer to work with the Privacy Commissioner on a collaborative basis to help them better understand what is and is not required in order to achieve reasonable and appropriate privacy protection. A focus on working with parties to resolve issues is seen as more productive than a complaint-based approach that is adversarial in nature and directed only towards enforcing a charge of a breach of the Act.

John Gustavson of the Canadian Marketing Association had this to say about the benefits of the ombudsman model:

> The evidence of the past few years clearly indicates that the ombudsman model has worked very well in promoting and protecting the privacy rights of Canadians. In response to complaints, organizations have invariably demonstrated a willingness to follow the direction of the Privacy Commissioner. We also feel that the commissioner's role as a privacy advocate is one that inherently contains positional bias and is therefore more compatible with an ombudsman's role. Most importantly, however, the reality is that the commissioner's powers of influence are well supported by the discretionary power to publicize privacy breaches and by the ability to seek binding orders through the Federal Court. (December 4, 2006)

For her part, the Federal Privacy Commissioner made it clear that she was not seeking any changes to her powers at this time.

> In our view, now is not the best time to move on the order-making power issue. The Office of the Privacy Commissioner has tried to do its job over the last three-and-a-half years in an atmosphere of instability, constant and detailed scrutiny and reduced administrative capacity. We are just emerging from this period, renewed, rehabilitated

> and having received sufficient resources. In our view, the administrative consequences of introducing an order-making power at this time would reduce the efficiency of the OPC in carrying out its multi-faceted mandate (November 27, 2006, brief, p. 6)

Moreover, the Commissioner has indicated that the Act has not been in force long enough for her to utilize all the powers of enforcement available to her. For example, she has yet to explore the potential to seek damage awards before the Federal Court, the extent of her auditing powers has yet to be tested, and there are penal provisions under the Act that have not yet been used.

In view of the concerns raised by the Federal Privacy Commissioner, this Committee believes that now is not the time to make changes to the Commissioner's enforcement powers under the Act. We feel that there is merit in the ombudsman approach in terms of ensuring the compliance of organizations that are subject to privacy complaints. Moreover, we agree that it would be premature to consider adding order-making to the Commissioner's enforcement powers before she has had a chance to more fully explore and make greater use of all her existing powers under the law.

The Committee acknowledges that there may come a time in the future when it may be necessary to recommend such order-making powers be granted to the Commissioner if further experience demonstrates that the Commissioner's existing powers prove insufficient to properly administer respect for, and compliance with, the Act. The Committee is also mindful of the fact that any consideration of changes to the powers of the Privacy Commissioner must be studied carefully in the context of the interrelationship between her office and that of the Information Commissioner of Canada, and we flag this point for any future study of this issue.

Recommendation 18

The Committee recommends that the Federal Privacy Commissioner not be granted order-making powers at this time.

2. Naming Names

Currently, section 20(1) of PIPEDA obliges confidentiality on the part of the Commissioner, or any person acting on her behalf or under her direction, with respect to information that comes to their knowledge as a result of the performance of their duties under the Act. Subsection 20(2), however, allows the Commissioner to make public any information relating to the personal information management practices of an organization, if the Commissioner considers that it is in the public interest to do so. It is this limited exemption that was the focus of testimony by witnesses before this Committee.

Many privacy advocates called upon the Committee to amend PIPEDA to require the Commissioner to publicly name all organizations that have been found to have violated the Act. It was argued, for example, that organizations should be held publicly accountable for their actions and that if there are no order-making powers to ensure compliance, then the public should be able to hold violators accountable. Philippa Lawson, of the Canadian Internet Policy and Public Interest Clinic (CIPPIC), made her argument in the following terms:

> The Office of the Privacy Commissioner is being far too reluctant to use the powers of her office that she does have. Chief amongst these is the power to make any information gathered in her inquiries under the act public, if it is in the public interest. And this is subsection 20(2). The Commissioner has effectively indicated that she will never use it. Maybe, just maybe, she will for repeat offenders. [...] However, if consumers are to have any effect on the bad actors in the industry on the subject of privacy, they must be able to express their displeasure to the company involved. This cannot be done when the company is protected from any adverse publicity or consumer action. If this committee does not recommend full order-making power for the commission, then at the least we are calling for you to ask that the present section 20 of PIPEDA be reviewed and amended to direct the publication of names of respondents. (December 6, 2006)

Organizations, on the other hand, felt that the Commissioner's power in this respect should remain discretionary. The naming of every organization in every instance where there has been a finding of non-compliance by the Commissioner could be injurious to a business' reputation and, in fact, mislead consumers (i.e. in instances of a minor error that has been corrected with no harm to the consumer or where the issue involves only one arm of a large corporation). Ariane Siegel, for the Information Technology Association of Canada (ITAC), argued:

> Currently, case summaries are reported for the most part on an anonymous basis. The Commissioner has taken the position that naming respondents in each and every case would not meet the public interest threshold of the legislation. ITAC supports this approach. The Commissioner has the discretion she requires in order to name respondents. ITAC believes that a mandatory practice of naming respondents in each and every instance would not benefit parties to any dispute, and, in fact, could result in negative consequences. Complaint resolution often results in a change to business policies or procedures such that the benefit naturally accrues to all customers. In this way, positive results are achieved with a high degree of efficiency. (December 11, 2006)

Although the Commissioner did not provide the Committee with detailed recommendations on this matter, she did provide an article she wrote that outlines her position on naming organizations under PIPEDA.[28] The Commissioner stresses the obligation of confidentiality as being integral to the ombudsman approach in that it enables complainants to be more forthcoming, open and vulnerable, while at the same time allowing respondents to be self-critical and willing to espouse a change of practice. That

---

[28] Jennifer Stoddart, "Cherry Picking Among Apples and Oranges: Refocusing Current Debate About the Merits of the Ombuds-Model under PIPEDA", *Canadian Business Law Journal*, Volume 44, No. 1 pp. 9-12.

being said, she acknowledges that the Act does provide for an exception to the confidentiality rule where it is in the public interest. Given that this is a limited exception, she sets out a number of criteria that should apply to its application. For example, decisions to disclose should be on a case by case basis, there must be some reason for the disclosure which is rationally connected to the purpose for which the discretion is granted, and the extent of the disclosure should be limited to that information necessary to meet the specified purpose.

For many of the same reasons given with respect to the issue of order-making powers, this Committee feels that now is not the time to alter the naming power of the Commissioner. The Committee supports the Commissioner's approach to the use of her discretionary powers under section 20(2), and recommends that no changes be made to the Act in this regard.

Recommendation 19

The Committee recommends that no amendment be made to section 20(2) of PIPEDA with respect to the Privacy Commissioner's discretionary power to publicly name organizations in the public interest.

3. Sharing Information with other Data Authorities

As noted with respect to the issue of naming names, the Privacy Commissioner is generally required to treat as confidential any information that is obtained in the exercise of her powers. In other words, the Office is not permitted, except in certain limited circumstances, to share information about a complainant without his or her consent. Section 23 of PIPEDA does allow the Commissioner to consult with any person whose powers and duties under substantially similar provincial legislation are like those of the Commissioner. This means that the Commissioner is able to share information and cooperate in investigations of mutual interest with her counterparts in Ontario (only with respect to Ontario health information), Alberta, British Columbia and Quebec. This power does not, however, extend to cooperative efforts with respect to data protection authorities in any other provinces or jurisdictions. The Commissioner is seeking an amendment to PIPEDA to grant her this specific authority.

According to testimony provided by the Privacy Commissioner, in view of the fact that we now live in a world of increasingly virtual borders where privacy issues know no national boundaries, it is imperative that data protection authorities have the ability to work together with consumer protection and other enforcement bodies on issues of mutual concern. Apparently, many data protection authorities around the world are already looking at ways in which they can work in closer contact. By way of example, the Commissioner is currently chairing an Organization for Economic Co-operation and Development (OECD) group that is exploring ways to encourage cooperation between data protection authorities and other enforcement bodies with respect to cross-border complaints and cases arising

from transborder data flows. The U.S. Federal Trade Commission also now has the ability to share confidential information with foreign law enforcers, subject to appropriate confidentiality assurances.

The Commissioner was supported in her request by other witnesses, in particular, the Information and Privacy Commissioner for British Columbia, David Loukidelis, who felt that the Federal Commissioner should have explicit authority for cooperative investigation, enforcement and other activities with privacy commissioners and data protection authorities outside Canada, particularly in Asia-Pacific region, the United States and the European Union.[29]

The Committee agrees that in a networked global economy, privacy issues are no longer isolated incidents within provincial or national borders. At a time of increasing trans-border information sharing, protecting the personal information of Canadians may require protection mechanisms both within and outside of Canada. It would appear as well that work is already underway in terms of the creation of an international privacy protection framework as an extension of jurisdictional mechanisms. This Committee therefore recommends that consideration be given to including a provision within PIPEDA that would grant the Commissioner the authority to share personal information with her provincial counterparts that do not have substantially similar private sector legislation as well as with her international counterparts while cooperating on investigations of interest to Canadians.

In making this recommendation, the Committee is mindful of the concerns of Canadians with respect to the privacy protection of any personal information that crosses our borders. Specifically, there are concerns about the risks posed by transfers of personal information to the United States in view of the U.S. *Patriot Act*, which was passed in the wake of the events of September 11, 2001 as a means of increasing the U.S. government's ability to conduct searches and to seize or compel the disclosure of records. The Committee therefore recommends that the government also consider how information shared between data protection authorities can be adequately protected from disclosure to a foreign court or other government authority for purposes other than those for which it was shared.

Recommendation 20

The Committee recommends that the Federal Privacy Commissioner be granted the authority under PIPEDA to share personal information and cooperate in investigations of mutual interest with provincial counterparts that do not have substantially similar private sector legislation, as well as international data protection authorities.

---

[29] November 29, 2006, brief, p. 3.

Recommendation 21

The Committee recommends that any extra-jurisdictional information sharing, particularly to the United States, be adequately protected from disclosure to a foreign court or other government authority for purposes other than those for which it was shared.

4. Solicitor-Client Privilege

Under PIPEDA, individuals have a broad right of access to their personal information held by an organization; however, section 9 of the Act sets out a limited number of circumstances when an organization may refuse an access request. One exception to the access requirement is where the information is protected by solicitor-client privilege (section 9(3)(a) of PIPEDA). Where an organization seeks to withhold personal information on this basis, a complaint may be filed with the Privacy Commissioner who, in turn, is obliged to conduct an investigation of the matter. Pursuant to this investigation power, the Privacy Commissioner argues that she has a need to examine the documents for which solicitor-client privilege is claimed in order to determine whether they were properly withheld pursuant to the Act. It is a power that she currently has under section 34(2) of the *Privacy Act* and she testified that a similar provision was not added to PIPEDA because no one thought it would be a problem. The matter is currently before the courts.

The Privacy Commissioner specifically asked the Committee to address the impact of the recent Federal Court of Appeal decision in *Blood Tribe*[30], which could allow organizations to use any claim of solicitor-client privilege to prevent her from reviewing documents in the course of investigations. Pursuant to this decision, the Commissioner would not have the power to compel and review those documents in order to verify that they did, in fact, contain information subject to solicitor-client privilege. The Commissioner described her concern in the following words:

> I'd like to raise one very specific and I think pressing matter that relates to a recent Federal Court of Appeal decision. This case deals with solicitor-client privilege and our ability to obtain access to documents in the course of our investigations. This recent decision in the Blood Tribe case leaves a gaping hole in our ability to conduct meaningful investigations. It effectively allows organizations to shield information from our investigators with no independent verification that the documents in question do in fact contain information subject to solicitor-client privilege. Although we are seeking leave to appeal, we believe this ambiguity in the legislation needs to be clarified with an amendment to PIPEDA as soon as possible. (November 27, 2006)

---

30 *Blood Tribe Department of Health v. Privacy Commissioner of Canada*, (2006) FCA 334, Fed. CA, reversing *Blood Tribe Department of Health v. Canada (Privacy Commissioner)* (2005) 40 CPR (4th) 7, Fed. Ct. (TD).

In the *Blood Tribe* case, the Federal Court of Appeal considered the power of the Commissioner to compel the production of documents in respect of which solicitor-client privilege was claimed, and found that Parliament, in enacting PIPEDA, had not intended the Commissioner's investigative powers to be unfettered by questions of solicitor-client privilege. The Court held that express statutory language would be required to abrogate solicitor-client privilege, and in the absence of such language, the Commissioner did not have the power to compel production of the documents in order to verify the claim of privilege. The Court noted that in cases where a broad claim of solicitor-client privilege is used as a shield to thwart an investigation, the Commissioner has the power to go to the Federal Court under section 15 of PIPEDA and have the claim of privilege reviewed by a Federal Court judge.

Vivian Bercovici, for the Dominion of Canada General Insurance Company, supported the decision of the Federal Court of Appeal in *Blood Tribe* and argued strongly against the amendment being sought by the Privacy Commissioner:

> [S]olicitor-client privilege goes to the heart of the order and integrity of our system of justice. An individual or party in any proceeding must know with confidence that any communication with their solicitor will not be disclosed. This allows free and unthreatened communication between solicitor and client, which facilitates the preparation and execution of a full and vigorous defence. The impact of qualifying solicitor-client privilege, which has anchored a common law tradition for centuries, would be seismic (February 6, 2007)

The Committee is in agreement with the Commissioner that there should be a means of independently verifying the appropriateness of a claim of solicitor-client privilege in respect of the denial of access to personal information under section 9 of PIPEDA. However, we disagree that the verification should stem from the Commissioner's investigative process and powers. We are also not convinced that section 15 of PIPEDA currently provides an avenue for the Commissioner to challenge a claim of solicitor-client privilege before the Federal Court in cases where she is unable to review the documents at issue. We therefore recommend that PIPEDA be amended to permit the Privacy Commissioner to apply for an expedited review of the claim of solicitor-client privilege by a judge of the Federal Court. If the judge determines that the claim of solicitor-client privilege was improperly invoked, then the Court could order that the documents at issue be produced to the individual.

The Committee recognizes that its recommendation in this context will result in an approach that is different from that taken under the *Privacy Act;* however, given that PIPEDA is different in origin and purpose from the federal public sector law, we do not feel obliged to import principles from the latter into the former.

Recommendation 22

The Committee recommends that PIPEDA be amended to permit the Privacy Commissioner to apply to the Federal Court for an expedited review of a claim of solicitor-client privilege in respect of the denial of access to personal information (section 9(3)(a)) where the Commissioner has sought, and been denied, production of the information in the course of an investigation.

BREACH NOTIFICATION

An issue addressed by most of our witnesses was the question of an organization's duty to notify individuals in instances of security breaches of personal information holdings. Currently, notification is voluntary, although the Committee was told that, in practice, organizations often consult the Office of the Privacy Commissioner in order to determine whether and, if so, how to notify their customers that a breach has occurred. Business response to security breaches can therefore vary widely, depending on factors such as the number of individuals affected, the nature of the information that was lost, and the likelihood that it could be accessed by someone who would use it for wrongful purposes. As more stories of major breaches involving the personal information of large numbers of Canadians are covered in our daily newspapers, concern about this issue is growing.

Many U.S. states have passed legislation requiring that customers be notified when their personal information has been compromised. These laws typically provide for large fines for failure to notify. In Canada, only Ontario's *Personal Health Information Protection Act* requires notification after a security breach. That Act requires health information custodians to notify individuals at the first reasonable opportunity if their personal health information is stolen, lost, or accessed by unauthorized persons.[31]

Businesses, for the most part, feel that they already have a duty to notify individuals in instances of significant security breaches involving personal information. They note that the Openness Principle (Principle 8) of the CSA Model Code, which is found in Schedule 1 of PIPEDA, suggests that organizations have responsibilities along these lines and consequently, there is no need for specific legislative provisions at this time. The Canadian Life and Health Insurance Association Inc. outlined its self-assessed, risk-based approach to notification:

> The industry supports a risk-based approach to notification, where the need to notify and the method of notifying the individual are proportional to the risk of harm that may be experienced by those whose personal information has been compromised. Under such an approach, any notification requirement would only be necessary where the breach is

---

31 Section 12(21)

material; where the organization has reasonable grounds to believe that disclosure of personal information to unauthorized individuals has taken place; and, where the disclosure presents a significant risk of harm to individuals (e.g. identity theft or fraud). (February 1, 2007, brief, pp. 11-12.)

Industry groups were generally supportive of guidance provided by the Privacy Commissioners of Canada, British Columbia and Ontario. The Ontario and British Columbia Information and Privacy Commissioners have together issued a *Breach Notification Assessment Tool*[32] to assist organizations in determining what steps should be taken in the event of a privacy breach. The Federal Commissioner and her office are also working with industry to develop voluntary guidelines to govern organizations' responses to security breaches. As the Committee was told by David Elder, of the Canadian Chamber of Commerce:

> The Canadian Chamber does not believe that mandatory breach notification is necessary in the legislation. We would encourage businesses to continue to work closely with the Privacy Commissioner's office in order to identify breaches and to notify those who could be affected by a possible breach in privacy. This flexibility enables notice where appropriate in the circumstances, with no adverse impact on consumers. I'd also like to note that it would be beneficial for the Canadian Chamber and other business associations to develop a best practices set of guidelines that could be used when breaches in privacy occur. To that end, business groups, including the Canadian Chamber, ITAC, the CMA, and others, are currently developing breach notification guidelines in conjunction with the Office of the Privacy Commissioner. Details on these best practices guidelines should be available later this spring. (February 1, 2007)

Those who argued in favour of a mandatory breach notification provision in PIPEDA spoke of the need to inform consumers in order for them to be able to effectively fight the increasing incidents of identity theft in this country. In its brief to the Committee, the Public Interest Advocacy Centre had this to say:

> The only way true accountability can be achieved is by imposing upon every organization a legal obligation to report any data leak to the OPCC and to notify all individuals whose personal information has been the subject of a security breach. Furthermore, this notification should not be qualified or diluted in any way. Every time the security of someone's personal information is breached, it should be incumbent upon the organization charged with securing and protecting that information to inform the individual of the breach. This provides every individual the autonomy to make their own decision concerning what measures to take next. It should not be up to the organization to unilaterally decide the level of risk caused by the breach or the severity of the potential harm. (October 23, 2006, p. 19)

---

[32] B.C. and Ontario Information and Privacy Commissioners, *Breach Notification Assessment Tool*, December 2006, http://www.ipc.on.ca/images/Resources/up-ipc_bc_breach.pdf.

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) issued a White Paper on Breach Notification[33] that makes specific recommendations for amending PIPEDA. The paper calls for a Canadian law requiring organizations to notify individuals when their personal information has been compromised as a result of a breach of the organization's security. In particular, it calls for an amendment to PIPEDA to provide for mandatory notification of security breaches when certain types of personal information are exposed to unauthorized access as a result of a security breach. The White Paper analyzes, and in some cases adopts, certain aspects of security breach legislation in the United States, where over half the states have enacted a mandatory security breach disclosure requirement, and where several federal bills are currently pending.

Privacy expert, Murray Long, also provided the Committee with a specific four-point proposal for breach notification. First, there should be a duty to notify that would apply to all types of sensitive information, not just financial data. Second, organizations should have some discretion to determine when to notify the public, but that should be based upon their self-assessment and an objective standard, to ensure that organizations act prudently. The objective standard would require that organizations notify the Privacy Commissioner when a reasonable person would consider it appropriate to do so, and that they do so within a short, legally-prescribed timeframe. Third, when they notify the Privacy Commissioner, organizations would be required to describe the impacts of the breach, the efforts taken to mitigate it, and what decision was made to notify affected persons. If they decided not to notify persons, they would be required to explain that decision, and the Privacy Commissioner could then evaluate their decision. Fourth, it should be an offence under the Act to fail to disclose notice of a breach where a reasonable person would expect that disclosure to have taken place.[34]

The Information and Privacy Commissioner for British Columbia, David Loukidelis, cautioned against following the notification requirements adopted in some U.S. jurisdictions, arguing that there is no evidence available yet to demonstrate that mandatory notification is actually a cost-effective way to reduce the risk of identity theft related to security breaches.

In her initial appearance before the Committee, the Federal Privacy Commissioner was also cautious in her approach to this issue. While supporting the notion of a duty to notify, the Commissioner pointed to the difficulty of choosing an appropriate model and she noted that a duty to notify did not easily fit into the current PIPEDA model since there is no straightforward way to penalize organizations that fail to notify individuals about security breaches. The Commissioner did, however, recommend that in addition to adding a duty to notify, or as an alternative, a provision could be added to PIPEDA which would allow an

---

33 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper*, January 9, 2007, http://www.cippic.ca/en/bulletin/BreachNotification_9jan07-web.pdf.

34 Another element of Mr. Long's proposed model would be to amend the whistleblower rights section of the Act to include good faith disclosures of breaches as protected rights of employees.

organization that has suffered a security breach to notify credit bureaus about the breach and the individuals affected without the consent of those individuals. This would allow credit bureaus to be more proactive in protecting consumers from identity theft and fraud.

In her final appearance before the Committee, however, the Privacy Commissioner indicated that several recent major security breaches have generated an urgency to resolve this issue and as a result, the Commissioner is now recommending an amendment to PIPEDA to create a breach notification provision. Until such an amendment is made, the Commissioner will continue to work with stakeholders to develop voluntary guidelines. When questioned about her position on this issue by Committee Members, the Commissioner indicated that she did not feel that the introduction of an amendment to PIPEDA would greatly alter what is the current practice of organizations that are faced with a data security breach.

The Committee feels that there is a need for an amendment to PIPEDA to include a breach notification provision; however, we recognize that this will not be an easy task. We favour a model whereby organizations would be required to report breaches to the Privacy Commissioner, who would then conduct an analysis to determine whether or not notification should be made. Most critical in the development of a statutory breach notification model will be the necessary determination of threshold issues.

The Committee heard testimony that some form of standard should be established for notification that would take into consideration the nature and scope of the breach. For example, CIPPIC advocated for the California legislative model wherein the duty to notify is only triggered when there is an acquisition or reasonable belief of acquisition by an unauthorized person. It was felt that this standard is higher than mere access by an unauthorized person, but lower than a standard that requires notification if there is a risk of identity theft. The Canadian Bar Association recommended that a balanced privacy breach notification requirement be considered, such as a duty to notify only where an organization is not covered by security mechanisms (e.g. encryption or de-identification), or has received notice that such protection mechanisms have been breached and the information that has been compromised is sensitive personal information.

The Committee recognizes that the issue of threshold applies to two aspects of our recommended model: 1) the question of when organizations are required to report breaches to the Privacy Commissioner; and 2) the Commissioner's determination of whether or not there should be a notification. In determining the former threshold, we do not wish to see the Office of the Privacy Commissioner overburdened with breach reporting. Certainly, requiring notification to the Office of the Privacy Commissioner in every instance of a security breach may create an unworkable burden on that Office, and, at least, will have significant resource implications. We suggest that careful consideration be given to this issue in the development of a breach notification provision in PIPEDA.

Therefore, the Committee does not support what some refer to as "mandatory breach notification", in the sense of requiring that every person whose personal information

is compromised be notified in every case of a breach. We support requiring organizations to notify the Privacy Commissioner of certain defined security breaches, so that her office has an opportunity to assist in the determination of whether affected individuals should be notified, and if so, in what manner. This second stage of the process would be discretionary, in that the Privacy Commissioner would determine on a case by case basis whether or not to recommend notification.

In determining the specifics of an appropriate notification model for PIPEDA, the Committee believes that consideration should be given to threshold issues, such as under what conditions breaches of personal information holdings would be required to be reported to the Privacy Commissioner, as well as under what conditions the Privacy Commissioner would require notification of such reported breaches. There must also be consideration of questions of timing, manner of notification, penalties for failure to notify, and the need for a "without consent" power to notify credit bureaus in order to help protect consumers from identify theft and fraud.

Recommendation 23

The Committee recommends that PIPEDA be amended to include a breach notification provision requiring organizations to report certain defined breaches of their personal information holdings to the Privacy Commissioner.

Recommendation 24

The Committee recommends that upon being notified of a breach of an organization's personal information holdings, the Privacy Commissioner shall make a determination as to whether or not affected individuals and others should be notified and if so, in what manner.

Recommendation 25

The Committee recommends that in determining the specifics of an appropriate notification model for PIPEDA, consideration should be given to questions of timing, manner of notification, penalties for failure to notify, and the need for a "without consent" power to notify credit bureaus in order to help protect consumers from identity theft and fraud.

Recommendation 1

The Committee recommends that a definition of "business contact information" be added to PIPEDA, and that the definition and relevant restrictive provision found in the Alberta *Personal Information Protection Act* be considered for this purpose.

Recommendation 2

The Committee recommends that PIPEDA be amended to include a definition of "work product" that is explicitly recognized as not constituting personal information for the purposes of the Act. In formulating this definition, reference should be added to the definition of "work product information" in the British Columbia *Personal Information Protection Act,* the definition proposed to this Committee by IMS Canada, and the approach taken to professional information in Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector.*

Recommendation 3

The Committee recommends that a definition of "destruction" that would provide guidance to organizations on how to properly destroy both paper records and electronic media be added to PIPEDA.

Recommendation 4

The Committee recommends that PIPEDA be amended to clarify the form and adequacy of consent required by it, distinguishing between express, implied and deemed/opt-out consent. Reference should be made in this regard to the Alberta and British Columbia *Personal Information Protection Acts.*

Recommendation 5

The Committee recommends that the Quebec, Alberta and British Columbia private sector data protection legislation be considered for the purposes of developing and incorporating into PIPEDA an amendment to address the unique context experienced by federally regulated employers and employees.

Recommendation 6

The Committee recommends that PIPEDA be amended to replace the "investigative bodies" designation process with a definition of "investigation" similar to that found in the Alberta and British Columbia *Personal Information Protection Acts* thereby allowing for the collection, use and disclosure of personal information without consent for that purpose.

Recommendation 7

The Committee recommends that PIPEDA be amended to include a provision permitting organizations to collect, use and disclose personal information without consent, for the purposes of a business transaction. This amendment should be modeled on the Alberta *Personal Information Protection Act* in conjunction with enhancements recommended by the Privacy Commissioner of Canada.

Recommendation 8

The Committee recommends that an amendment to PIPEDA be considered to address the issue of principal-agent relationships. Reference to section 12(2) of the British Columbia *Personal Information Protection Act* should be made with respect to such an amendment.

Recommendation 9

The Committee recommends that PIPEDA be amended to create an exception to the consent requirement for information legally available to a party to a legal proceeding, in a manner similar to the provisions of the Alberta and British Columbia *Personal Information Protection Acts*.

Recommendation 10

The Committee recommends that the government consult with the Privacy Commissioner of Canada with respect to determining whether there is a need for further amendments to PIPEDA to address the issue of witness statements and the rights of persons whose personal information is contained therein.

Recommendation 11

The Committee recommends that PIPEDA be amended to add other individual, family or public interest exemptions in order to harmonize its approach with that taken by the Quebec, Alberta and British Columbia private sector data protection Acts.

Recommendation 12

The Committee recommends that consideration be given to clarifying what is meant by "lawful authority" in section 7(3)(c.1) of PIPEDA and that the opening paragraph of section 7(3) be amended to read as follows: "For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization shall disclose personal information without the knowledge or consent of the individual but only if the disclosure is [...]"

Recommendation 13

The Committee recommends that the term "government institution" in sections 7(3)(c.1) and (d) be clarified in PIPEDA to specify whether it is intended to encompass municipal, provincial, territorial, federal and non-Canadian entities.

Recommendation 14

The Committee recommends the removal of section 7(1)(e) from PIPEDA.

Recommendation 15

The Committee recommends that the government examine the issue of consent by minors with respect to the collection, use and disclosure of their personal information in a commercial context with a view to amendments to PIPEDA in this regard.

Recommendation 16

The Committee recommends that no amendments be made to PIPEDA with respect to transborder flows of personal information.

Recommendation 17

The Committee recommends that the government consult with members of the health care sector, as well as the Privacy Commissioner of Canada, to determine the extent to which elements contained in the PIPEDA Awareness Raising Tools document may be set out in legislative form.

Recommendation 18

The Committee recommends that the Federal Privacy Commissioner not be granted order-making powers at this time.

Recommendation 19

The Committee recommends that no amendment be made to section 20(2) of PIPEDA with respect to the Privacy Commissioner's discretionary power to publicly name organizations in the public interest.

Recommendation 20

The Committee recommends that the Federal Privacy Commissioner be granted the authority under PIPEDA to share personal information and cooperate in investigations of mutual interest with provincial counterparts that do not have substantially similar private sector legislation, as well as international data protection authorities.

Recommendation 21

The Committee recommends that any extra-jurisdictional information sharing, particularly to the United States, be adequately protected from disclosure to a foreign court or other government authority for purposes other than those for which it was shared.

Recommendation 22

The Committee recommends that PIPEDA be amended to permit the Privacy Commissioner to apply to the Federal Court for an expedited review of a claim of solicitor-client privilege in respect of the denial of access to personal information (section 9(3)(a)) where the Commissioner has sought, and been denied, production of the information in the course of an investigation.

Recommendation 23

The Committee recommends that PIPEDA be amended to include a breach notification provision requiring organizations to report certain defined breaches of their personal information holdings to the Privacy Commissioner.

Recommendation 24

The Committee recommends that upon being notified of a breach of an organization's personal information holdings, the Privacy Commissioner shall make a determination as to whether or not affected individuals and others should be notified and if so, in what manner.

Recommendation 25

The Committee recommends that in determining the specifics of an appropriate notification model for PIPEDA, consideration should be given to questions of timing, manner of notification, penalties for failure to notify, and the need for a "without consent" power to notify credit bureaus in order to help protect consumers from identity theft and fraud.

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the Committee requests that the government table a comprehensive response to this Report.

Respectfully submitted,

Tom Wappel, MP
Chairman

APPENDIX A
LIST OF WITNESSES

Organizations and Individuals	Date	Meeting
Department of Industry Michael Binder, Assistant Deputy Minister, Spectrum, Information Technologies and Telecommunications	2006/11/20	17
Department of Industry Danièle Chatelois, Privacy Policy Analyst, E-Commerce Policy Directorate, Electronic Commerce Branch	2006/11/20	17
Department of Industry Richard Simpson, Director General, Electronic Commerce	2006/11/20	17
Department of Justice Alexia Taschereau, Senior Counsel, Industry Canada	2006/11/20	17
As an Individual Colin Bennett, Political Science Professor, University of Victoria	2006/11/22	18
B.C. Freedom of Information and Privacy Association (FIPA) Richard Rosenberg, President	2006/11/22	18
Office of the Privacy Commissioner of Canada Jennifer Stoddart, Privacy Commissioner	2006/11/27	19
Office of the Privacy Commissioner of Canada Heather Black, Assistant Commissioner (PIPEDA)	2006/11/27	19
Office of the Privacy Commissioner of Canada Melanie Millar-Chapman, Strategic Research and Policy Analyst	2006/11/27	19
As an Individual Valerie Steeves, Department of Criminology, University of Ottawa	2006/11/29	20
Office of the Information and Privacy Commissioner of British Columbia David Loukidelis, Commissioner	2006/11/29	20
Canadian Marketing Association John Gustavson, President and Chief Executive Officer	2006/12/04	21
Canadian Marketing Association Wally Hill, Vice President, Public Affairs and Communications	2006/12/04	21

Organizations and Individuals	Date	Meeting
Canadian Marketing Association Barbara Robins, Vice-President, Legal and Regulatory Affairs, Reader's Digest	2006/12/04	21
Federally Regulated Employers - Transportation and Communication (FETCO) Don Brazier, Executive Director	2006/12/04	21
Federally Regulated Employers - Transportation and Communication (FETCO) Barbara Mittleman, Director, Employee Relations, Canadian Pacific Railway Company	2006/12/04	21
Federally Regulated Employers - Transportation and Communication (FETCO) Edith Cody-Rice, Senior Legal Counsel, Privacy Coordinator Canadian Broadcasting Corporation	2006/12/04	21
Canadian Internet Policy and Public Interest Clinic Philippa Lawson, Executive Director	2006/12/06	22
Marketing Research and Intelligence Association David Stark, MRIA Standards Chair	2006/12/06	22
Marketing Research and Intelligence Association Brendan Wycks, Executive Director	2006/12/06	22
Public Interest Advocacy Centre John Lawford, Counsel	2006/12/06	22
Public Interest Advocacy Centre Amanda Tait, Articling Student	2006/12/06	22
As an Individual Ian Kerr, Canada Research Chair in Ethics, Law and Technology, University of Ottawa	2006/12/11	23
Canadian Bar Association Brian Bowman, Chair, National Privacy and Access Law Section	2006/12/11	23
Canadian Bar Association Tamra Thomson, Director, Legislation and Law Reform	2006/12/11	23
Information Technology Association of Canada Bernard Courtois, President and Chief Executive Officer	2006/12/11	23
Information Technology Association of Canada Ariane Siegel, Lawyer	2006/12/11	23

Organizations and Individuals	Date	Meeting
Canadian Dental Association Wayne Halstrom, President	2006/12/13	25
Canadian Dental Association Andrew Jones, Director, Corporate and Government Relations	2006/12/13	25
Canadian Medical Association Bonnie Cham, Chair, Committee on Ethics	2006/12/13	25
Canadian Medical Association Jean Nelson, Assistant Director, Legal Services and Chief Privacy Officer	2006/12/13	25
Canadian Pharmacists Association Jeff Poston, Executive Director	2006/12/13	25
Canadian Bankers Association Terry Campbell, Vice-President, Policy	2007/01/30	26
Canadian Bankers Association Warren Law, Senior Vice-President, Corporate Operations and General Counsel	2007/01/30	26
Canadian Bankers Association Linda Routledge, Director, Consumer Affairs	2007/01/30	26
Credit Union Central of Canada Gary Rogers, Vice-President, Financial Policy	2007/01/30	26
Credit Union Central of Canada Charlene Loui-Ying, General Counsel and Government Relations Officer Credit Union Central of British Columbia	2007/01/30	26
Canadian Chamber of Commerce Michael Murphy, Executive Vice-President, Policy	2007/02/01	27
Canadian Chamber of Commerce Chris Gray, Policy Analyst	2007/02/01	27
Canadian Chamber of Commerce David Elder, Vice-President, Regulatory Law, Bell Canada	2007/02/01	27

Organizations and Individuals	Date	Meeting
Canadian Life and Health Insurance Association Inc. Yves Millette, Senior Vice-President, Quebec Affairs	2007/02/01	27
Canadian Life and Health Insurance Association Inc. Dale Philp, Assistant Vice-President and Senior Counsel , Sun Life Financial	2007/02/01	27
Canadian Life and Health Insurance Association Inc. Frank Zinatelli, Vice-President and Associate General Counsel	2007/02/01	27
Dominion of Canada General Insurance Company Vivian Bercovici, Counsel	2007/02/06	28
Dominion of Canada General Insurance Company Ann MacKenzie, Privacy Officer	2007/02/06	28
Insurance Bureau of Canada Randy Bundus, Vice-President, General Counsel and Corporate Secretary	2007/02/06	28
Insurance Bureau of Canada Mark Yakabuski, Vice-President, Federal Affairs and Ontario	2007/02/06	28
Murray Long & Associates Murray Long, President	2007/02/06	28
IMS Health Canada Gary Fabian, Vice-President, Public Affairs and Corporate Relations	2007/02/08	29
IMS Health Canada Anita Fineberg, Corporate Counsel and Chief Privacy Officer, Canada and Latin America	2007/02/08	29
IMS Health Canada Léo-Paul Landry, Member, Medical Advisory Board	2007/02/08	29
National Association for Information Destruction - Canada Dave Carey, Chair	2007/02/08	29
National Association for Information Destruction - Canada Robert Johnson, Executive Director	2007/02/08	29
Canadian Association of Chiefs of Police Clayton Pecknold, Co-Chair, Law Amendments Committee	2007/02/13	30

Organizations and Individuals	Date	Meeting
Canadian Resource Centre for Victims of Crime Steve Sullivan, President	2007/02/13	30
Canadian Resource Centre for Victims of Crime Krista Gray-Donald, Director of Research	2007/02/13	30
Insurance Brokers Association of Canada Robert Kimball, Chairman	2007/02/13	30
Insurance Brokers Association of Canada Peter Fredericks, Vice-President	2007/02/13	30
Insurance Brokers Association of Canada Steve Masnyk, Manager of Communications	2007/02/13	30
Canadian Federation of Independent Business Lucie Charron, Policy Analyst	2007/02/15	31
Canadian Federation of Independent Business Corinne Pohlmann, Director, National Affairs	2007/02/15	31
Consumers' Association of Canada Margaret Anne Ireland, Director	2007/02/15	31
Royal Canadian Mounted Police Bruce Rogerson, Assistant Commissioner	2007/02/20	32
Royal Canadian Mounted Police Art Crockett, Officer in Charge, Strategic Services Branch,Technical Operations	2007/02/20	32
Royal Canadian Mounted Police Earla-Kim McColl, Superintendent, National Child Exploitation Coordination Centre	2007/02/20	32
Office of the Privacy Commissioner of Canada Jennifer Stoddart, Privacy Commissioner	2007/02/22	33
Office of the Privacy Commissioner of Canada Heather Black, Assistant Commissioner (PIPEDA)	2007/02/22	33

APPENDIX B
LIST OF BRIEFS

Organizations and individuals

Advocis

Association of Canadian Archivists

B.C. Freedom of Information and Privacy Association (FIPA)

Burbidge, Scott

Canada Health Infoway

Canadian Bankers Association

Canadian Bar Association

Canadian Chamber of Commerce

Canadian Dental Association

Canadian Internet Policy and Public Interest Clinic

Canadian Life and Health Insurance Association Inc.

Canadian Marketing Association

Canadian Real Estate Association

Canadian Resource Centre for Victims of Crime

Credit Union Central of Canada

Federally Regulated Employers - Transportation and Communication (FETCO)

Federation of Medical Regulatory Authorities

IMS Health Canada

Information Technology Association of Canada

Insurance Bureau of Canada

Organizations and individuals

Kerr, Ian

Mouvement des caisses Desjardins

Murray Long & Associates

Mutual Fund Dealers Association of Canada

National Association for Information Destruction - Canada

Office of the Information and Privacy Commissioner of British Columbia

Office of the Privacy Commissioner of Canada

Public Interest Advocacy Centre

Royal Canadian Mounted Police

Speers, Richard

House of Commons Standing Committee on Access to Information, Privacy and Ethics (the "Committee")

Statutory Review of the *Personal Information Protection and Electronic Documents Act* (2000, c. 5) ("PIPEDA"): **DISSENTING OPINION**

The Conservative members of Committee acknowledge the thoughtful participation of the many individuals and groups who appeared as witnesses and/or presented submissions during the review. The majority report includes many constructive recommendations for technical changes, however, the Conservative members of the Committee dissent with recommendation 14 to repeal section 7(1)(e) of PIPEDA.

1.0 Listening to Small Business

As noted in the majority report, PIPEDA only fully came into effect on January 1, 2004. The Conservative members wish to emphasize the majority report's focus on fine-tuning PIPEDA, rather than prescribing wholesale changes. The business community, privacy stakeholders and officials, including the Office of Privacy Commissioner of Canada, are facilitating PIPEDA's adoption. The Conservative members of the Committee support those efforts. The Conservative members do not support efforts that would unduly increase the compliance burden on the small business community through, for example, changes that would make PIPEDA unnecessarily prescriptive. The Conservative members applaud the work of those business groups, including the Canadian Federation of Independent Business, helping small and medium-sized businesses comply with PIPEDA and protect Canadians' personal information.

2.0 Dissent

The Conservative members respectfully dissent from recommendation 14 of the majority report, and the reasons given at paragraphs 79 through 85 of the majority report.

Section 7(1)(e) allows organizations to collect and use information related to national security, defence, or international affairs. The previous Liberal government included this section in PIPEDA for the express purpose of closing legislative gaps relating to transportation and national security, specifically air travel. The Conservative members of Committee believe the removal of section 7(1)(e) could threaten the safety of Canada's civil aviation system.

3.0 Inappropriate Timing

The majority's reconsideration of section 7(1)(e) is premature. The section was adopted as part of the *Public Safety Act*, 2002 (2004, c. 15), and only came into force in May 2004. Arguably, section 7(1)(e) is not properly within the ambit of this statutory review. By mandating a five (5) year review, the drafters of PIPEDA determined stakeholders ought to actually benefit from five (5) years of experience before reflecting the efficacy of the legislation. Section 7(1)(e) was not part of the original legislation, so affected stakeholders have not benefited from five (5) years of experience with the provision.

4.0 No Stakeholder Input Before the Committee

The *Public Safety Act* was the product of an attempt to balance public safety and individual privacy. In contrast, the majority report recommends repealing part of the *Public Safety Act* without any input from the affected stakeholders, including airlines, airports, air passenger groups or security agencies. Recommendation 14 and paragraphs 79-85 of the majority report are completely devoid of input from the stakeholders most affected by the recommendation.

The Conservative members of the Committee note that, notwithstanding any comments in the majority report, the Honourable Stockwell Day, Minister of Public Safety and Emergency Preparedness, replied to the Committee in a letter dated April 19, 2007. The Conservative members of the Committee appreciate the input of the Minister on sections 7(1)(e) and 9. The Conservative members of the Committee also welcome the Minister's interest in clarifying section 7(3)(c.1). Minister Day's letter is attached as an annex to this dissenting opinion.

4.0 Conclusion

The Conservative members vigorously dissent from the majority's recommendation to weaken Canada's national security laws; a recommendation made by the Liberal and New Democrat members without any input or representation from the security or air transportation communities.

Minister of Public Safety
and Emergency Preparedness

Ministre de la Securite publique
et de la Protection civile

Ottawa, Canada K1A OP8

Mr. Tom Wappel, M.P.
Chairman
Standing Committee on
Access to Information, Privacy and Ethics
House of Commons
Ottawa, Ontario KIA OA6

Re: Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)

Dear Mr. Wappel

Thank you for your letter of March 20, 2007. I appreciate the opportunity to contribute to the House of Commons Standing Committee on Access to Information, Privacy and Ethics' important work in conducting a statutory review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

You requested my views on s. 7(1) (e) of PIPED A, which was added to PIPEDA by the *Public Safety Act.*

Subsection 7(1)(e) provides that an organization may collect personal information without the knowledge or consent of the individual if the collection is made for the purposes of a disclosure required by law or a disclosure to the government, where the information relates to national security, defence, or international affairs and is either requested by a government institution that has lawful authority to obtain it, or on the organization's own initiative.

Part of the objective of subsection 7(1)(e), as part of the *Public Safety Act* (which received Royal Assent on May 6,2004), is to improve Canada's capacity to provide a secure environment, in particular for transportation and air travel. The Act closes legislative gaps relating to transportation and national security by amending existing laws, such as the *Aeronautics Act,* the *Criminal Code,* the *Canadian Air Transport Security Authority Act,* and others, as well as PIPEDA.

The amendments to the *Aeronautics Act* in particular were designed to grant the authority to request, and use, passenger information to protect the security of the country and its aviation system. The amendments to PIPEDA s.7 (1) (e) and 7(2) (d) were consequential amendments needed to ensure that the provisions of PIPEDA did not conflict with the *Public Safety Act.*

It should also be noted that an important goal of the *Public Safety Act* is to balance the interest of public safety and individual privacy, and a number of safeguards were included in the law to achieve this, while ensuring transparency and accountability. The proposals were the subject of extensive consultations, and a lengthy review in Parliament. Many changes were made throughout this process to address comments and concerns expressed by various stakeholders, including the Office of the Privacy Commissioner and, as a result, the amendments to PIPEDA provided for under s. 98 of the *Public Safety Act* are limited in scope and narrowly targeted to achieve their goals.

Given the above, I am concerned about the impact that changes suggested by witnesses to the previous PIPEDA amendments, enacted pursuant to the *Public Safety Act,* could have on achieving the goals of the *Public Safety Act* and, as a consequence, on public safety.

Strong safeguards in relation to law enforcement activities are already enshrined in legislation such as Police Acts and the *Criminal Code,* to review the actions of the police when collecting and using personal information. In addition, the court system oversees the results of police work and ensures, in applying the laws of evidence, as well as the *Charter of Rights and Freedoms,* that police collection of information is done appropriately.

As you know, PIPEDA was enacted to protect the privacy of information being held by private companies and was never intended to impede police work. However, the current wording of section 7 and section 9 of PIPEDA has led to confusion among the private sector as to how and whether they can cooperate with the police, which should be remedied.

Section 7:

Subsection 7(3)(c.1) states that an organization may disclose personal information without the knowledge or consent of the individual if the government institution has lawful authority to obtain the requested information. Unfortunately, the phrase "lawful authority" has been misinterpreted by some private sector organizations as an obligation to obtain judicial authorization before releasing any information to police and security agencies.

While the language of s. 7(3)(c), which refers to subpoenas and warrants, can clearly be considered to preclude such an interpretation oflawful authority under s.7(3)(c.!), the reality is that the lack of a definition of lawful authority has resulted in an ambiguity, which is in many instances posing a problem for police.

A requirement to obtain a warrant was never intended, nor would it be practical, given the broad definition of personal information. This misinterpretation can result in an inability for police to obtain even basic information needed for general policing functions to assist the public. A troubling example of the potential negative impact of a misinterpretation of this provision is seen in the context of an Internet Service Provider refusing to provide urgently necessary contact information on a subscriber to the police in a situation where a child is being lured in real-time in a chat room by an online predator.

Given the above challenges resulting from the lack of clarity as to what constitutes "lawful authority", I believe that this section, in particular the term "lawful authority", would benefit from clarification.

Section 9:

Section 9 of PIPEDA is also causing law enforcement agencies some concern, due to a possible loophole in the provision designed to protect police investigations. PIPEDA provides that an individual shall be given access to personal information about themselves and have a right to be informed about the disclosure of any of their personal information. To protect investigations, section 9 of PIPED A provides an exception whereby law enforcement agencies can object and thereby prohibit an organization from revealing to an individual that a request has been received from or disclosure of information has been provided to a law enforcement agency.

Section 9, however, does not address the situation where an organization chooses voluntarily to disclose to an individual a police request for information. Significant harm can result to ongoing police investigations if an organization voluntarily discloses to an individual that he or she is under investigation. For example, this individual or group could then proceed to destroy evidence before the police could intercede.

It is therefore important to police investigations that section 9 be clarified to ensure that organizations are prohibited from disclosing the existence of an investigation or the fact that the police had made any inquiries regardless of

whether an individual has made a request for this information or the organization wishes to voluntarily notify the individual.

I recently wrote to my colleague, the Honourable Maxime Bernier, Minister of Industry, to advise him of the challenges the police have experienced with respect to PIPEDA. I have attached a copy of my letter to him for your reference.

Thank you again for the opportunity to contribute to the Committee's work in reviewing this important piece of legislation.

Yours sincerely,

Stockwell Day, P.C., M.P.
Minister of Public Safety

Bloc Québécois Dissenting Report
April 23, 2007

The Bloc Québécois played an active and responsible role in the study of Part I of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Although we had suggested a number of amendments to "limit the damage," the Bloc Québécois wishes to reiterate its complete disagreement with this act, which was adopted in 2000 and was widely criticized by the Government of Québec, businesses, consumers, the Québec Employers' Council, editorial writers, constitutional experts, etc.

PIPEDA: an example of raiding by the federal government

Let us recall that the PIPEDA was passed during the controversy in the late 1990s, when Bill C-6[1] received royal assent. The Government of Québec and the provinces argued essentially that while the federal government claimed legitimacy for the PIPEDA pursuant to its jurisdiction over the regulation of trade and commerce, the protection of personal information falls under the jurisdiction of Québec and the provinces by virtue of the constitutional power over property and civil rights. In this regard, a constitutional expert from Québec noted:

> *"In my opinion, Bill C-54 violates the letter and the spirit of the division of powers as it must be understood in this country. It takes an arrogant and intrusive approach to provincial areas of jurisdiction. […] The protection of privacy is essentially a matter of provincial jurisdiction. In Québec, for instance, property and civil rights, the Civil Code and the Québec act apply, in addition to the Canadian and Québec charters."*
>
> Jacques Frémont, constitutional expert, Université de Montréal

In Québec, personal information is protected

The federal act merely overlaps with existing provisions in Québec:

- The *Act Respecting the Protection of Personal Information in the Private Sector* has protected personal information in Québec since 1993;
- The *Québec Charter of Rights* explicitly states in section 5 that every person has the right to privacy;
- The *Civil Code* (Chapter 3, especially sections 36 to 40) includes provisions regarding the protection of privacy.

Moreover, businesses under federal jurisdiction with dealings in Québec were already covered by the Québec act. Québeckers' right to the protection of privacy is protected by the Québec act, whether in dealings with a business under provincial or federal jurisdiction. The Task Force on the Future of the Canadian Financial Services Sector devoted an entire volume to the protection of personal

---

1 C-6 replaced Bill C-54, which died on the Order Paper in September 1999.

information in this sector, written by Richard Owen and published last September. It states:

> "On a literal reading, the Act applies to banks as well as other financial institutions. *(...) In the absence of federal legislation on a particular subject matter, validly enacted provincial law may apply to a federal undertaking unless the law prevents the federal undertaking from managing its operations or generally accomplishing its ends."*[2]

Moreover, the report states that Québec law already applied to interprovincial and international trade as well.

> "Moreover, the effects of the Québec Act will not be confined to the province. National institutions will face the Act's restriction on the extra-provincial transfer of information (about Québec residents)."[3]

The PIPEDA gives the federal government the power to render a Québec law invalid

The federal act applies to all financial activities unless the Governor in Council orders, if satisfied that a province has adopted similar legislation, that it be exempted in whole or in part.

In December 2003, the federal government issued an exclusion order[4] applicable to organizations in Québec. Unfortunately, not only is the power set out in paragraph 26(2)b[5] left to the government's sole discretion, but it applies only to information within Québec and held by companies under provincial jurisdiction.

Pursuant to this paragraph, the Governor in Council could therefore if it wishes order that the laws of Québec be declared partially or wholly invalid, without even referring the matter to Parliament. This is unacceptable to the Bloc Québécois.

---

2 Task Force on the Future of the Canadian Financial Services Sector. *Privacy and Financial Services in Canada,* Owens, Richard, September 1998, p. 79-80

3 Op. cit. , p. 82

4 http://canadagazette.gc.ca/partII/2003/20031203/html/sor374-e.html

5 26(2)(*b*) if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province.

sont protégés par la loi québécoise, qu'ils fassent affaire avec une entreprise de juridiction provinciale ou une entreprise de juridiction fédérale. Le Groupe de travail sur l'avenir du secteur des services financiers canadiens a consacré un volume à la protection des renseignements personnels dans ce secteur, rédigé par Richard Owen et publié en septembre dernier. On peut y lire :

> *« À la lecture du libellé de la Loi, on constate qu'elle s'applique autant aux banques qu'aux autres institutions financières. (…) En l'absence de lois fédérales en la matière, une loi adoptée par un gouvernement provincial pourrait s'appliquer à un domaine de compétence fédérale à moins qu'elle n'empêche le gouvernement fédéral d'accomplir les devoirs qui lui incombent habituellement. »*[2]

De plus, le rapport précise que la Loi québécoise s'appliquait aussi déjà au commerce interprovincial et international.

> *« En outre cette loi a des conséquences qui ne se limitent pas qu'au territoire québécois. Les institutions nationales établies un peu partout au pays devront composer avec ses dispositions en matière de transmission de renseignements personnels (concernant des résidants du Québec) à l'extérieur du Québec. »*[3]

La LPRPDE confère au gouvernement fédéral le pouvoir d'invalider une loi québécoise

La loi fédérale s'applique à l'ensemble des activités commerciales, à moins que le gouverneur en conseil décrète, s'il est convaincu qu'une province a adopté une loi essentiellement similaire, de l'exempter en tout ou en partie.

En décembre 2003, le gouvernement fédéral a pris un décret[4] d'exclusion visant des organisations du Québec. Malheureusement, non seulement ce pouvoir, prévu à l'article 26(2)b[5], est laissé à la seule discrétion du gouvernement, mais il ne concerne que les renseignements qui demeurent sur le territoire du Québec et qui sont gardés par des entreprises de juridiction provinciale.

Ainsi, par cet article, le gouverneur en conseil pourrait, par décret, décider s'il lui sied d'invalider complètement ou seulement en partie les lois du Québec, sans même en référer au Parlement. Le Bloc Québécois ne peut accepter une telle situation.

---

2 Le Groupe de travail sur l'avenir des services financiers canadiens .- *La protection des renseignements personnels dans le secteur des services financiers au Canada*, par OWENS, Richard, septembre 1998, p. 79-80

3 Op. cit. , p. 82

4 http://canadagazette.gc.ca/partII/2003/20031203/html/sor374-f.html

5 26(2)*b*) s'il est convaincu qu'une loi provinciale essentiellement similaire à la présente partie s'applique à une organisation — ou catégorie d'organisations — ou à une activité — ou catégorie d'activités — , exclure l'organisation, l'activité ou la catégorie de l'application de la présente partie à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels qui s'effectue à l'intérieur de la province en cause.

Rapport dissident du Bloc Québécois
23 avril 2007

Le Bloc Québécois a participé activement et de manière responsable à l'étude de la Partie 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Bien que nous ayons proposé certains aménagements afin de « limiter les dégâts », le Bloc Québécois tient à réitérer son total désaveu de cette loi, adoptée en 2000, et qui a été largement dénoncée par le gouvernement du Québec, les entreprises, les consommateurs, le Conseil du patronat, les éditorialistes, les constitutionnalistes, etc.

La LPRPDE : un exemple de prédation fédérale

Rappelons que la LPRPDE a été adoptée dans la controverse à la fin des années 1990, lorsque le projet de loi C-6[1] a reçu la sanction royale. Essentiellement, le gouvernement du Québec et les provinces ont plaidé que, bien que le gouvernement fédéral tente d'appuyer la légitimité de la LPRPDE sur sa compétence en matière de réglementation des échanges et du commerce, la protection des renseignements personnels relève du Québec et des provinces en vertu du pouvoir constitutionnel en matière de propriété et de droits civils. À ce sujet, voici ce que disait un constitutionnaliste québécois :

> *« Le projet de loi C-54, selon moi, viole l'esprit et la lettre du partage des compétences, tel qu'on doit le comprendre en ce pays. Il met de l'avant une approche arrogante et importune à l'égard des compétences provinciales. […] La protection de la vie privée est une compétence essentiellement de principe des provinces. Au Québec, par exemple c'est la propriété et les droits civils, c'est le Code civil, c'est la loi québécoise qui s'applique, en plus des chartes canadiennes et québécoises. »*
>
> Jacques Frémont, constitutionnaliste, Université de Montréal

Au Québec, les renseignements personnels sont protégés

Au Québec, la loi fédérale ne fait que chevaucher des dispositions existantes :

- la *Loi sur la protection des renseignements personnels dans le secteur privé* protège les renseignements personnels des Québécois depuis 1993;
- la *Charte québécoise des droits* reconnaît explicitement à son article 5 que toute personne a droit au respect de sa vie privée;
- le *Code civil* (chapitre 3, plus particulièrement les articles 36 à 40) contient des dispositions sur la protection de la vie privée.

De plus, notons que les entreprises de juridiction fédérale faisant affaire au Québec étaient déjà couvertes par la Loi québécoise. En effet, les droits des Québécoises et Québécois à la protection de leurs renseignements personnels

---

1 C-6 succédait au projet de loi C-54, mort au Feuilleton en septembre 1999.

personnels qui la concernent et a Ie droit d'etre informee de la divulgation de tout renseignement personnel â son sujet. Toutefois, afin de proteger les enquetes, l'article 9 de la LPRPDE etablit une exception suivant laquelle les organismes d'application de la loi peuvent s'opposer â ce qu'une organisation revele â la personne interessee qu'une demande a Me presentee par un organisme d'application de la loi ou que des renseignements ont ete communiques â cet orgamsme.

Toutefois, l'article 9 ne prevo it pas la situation ou une organisation decide de son plein gre de divulguer â la personne interessee une demande de renseignements de la police. Une organisation qui informe volontairement une personne interessee de la tenue d'une enquete peut ainsi nuire considerablement aux enquetes policieres en cours. De certe fayon, la personne ou Ie groupe interesse pourrait en suite detruire des elements de preuve avant que la police puisse intervenir.

II est done important pour les enquetes policieres de clarifier I' article 9 de fayon â interdire aux organisations de reveler I' existence d'une enquete ou Ie fait que la police a demande quelque renseignement que ce soit, independamment du fait que la personne interessee ait ou non presente une demande pour Hre informee d'une telle situation ou du fait que l'organisation souhaite de son plein gre informer la personne interessee.

J'ai recemment ecrit â mon collegue l'honorable Maxime Bernier, ministre de l'Industrie, pour l'aviser des difficultes que la LPRPDE occasionne aux policiers. J'ai annexe une copie de la lertre pour information.

Je vous remercie de nouveau de m'avoir offert l'occasion de contribuer aux travaux d'examen du Comite sur certe loi d'importance.

Je vous prie d'agreer, Monsieur Ie President, l'expression de mes sentiments distingues.
Stockwell Day, c.P., depute Ministre de la Securite publique

but de nuire au travail de la police. Cependant, Ie libelle actuel des articles 7 et 9 de la LPRPDEa cree une certaine confusion dans Ie secteur prive quant â savoir s'il est permis de collaborer avec la police et sur la fayon de Ie faire. II convient donc de dissiper cette confusion.

Article 7

L' alinea *7(3)c.1)* dispose qu 'une organisation peut communiquer des renseignements personnels â l'insu de l'interesse et sans son consentement si l'institution gouvernementale qui a demande Ie renseignement personnel a l' autorite legitime de l' obtenir. Malheureusement, Ie terme « autorite legitime» a ete mal interprete par certaines organisations du secteur prive, qui y ont vu une obligation d'obtenir une autorisationjudiciaire avant de communiquer toute information â la police et aux organismes de securite.

Bien que Ie langage de l'alinea *7(3)c),* qui fait etat d'assignation et de mandat, peut clairement etre compris comme excluant la possibilite que Ie terme « autorite legitime» â l'alinea *7(3)c.1),* soit mal interprete, dans les faits l'absence de definition d'« autorite legitime» a conduit â une ambigu'ite sur la teneur de cette notion. Or, dans bien des cas, cette ambigu'ite cause un probleme â la police.

Le legislateur n'ajamais eu l'intention d'exiger l'obtention d'un mandat. Une telle procedure ne serait pas pratique, compte tenu de la definition tres large de la notion de renseignements personnels. Cette interpretation erronee peut avoir pour effet d'empecher la police d'obtenir des renseignements elementaires dont elle a besoin pour remplir ses fonctions generales d' assistance au public. Un exemple inquietant des repercussions nefastes que risque d'entralner une interpretation erronee de cette disposition est celui du fournisseur de services Internet qui refuse de fournir d'urgence â la police les coordonnees essentielles d'un abonne, dans une situation OU un enfant est en train au moment meme d' etre pris au piege par un predateur en ligne dans un clavardoir.

Compte tenu des problemes que pourrait poser ce manque de clarte quant â ce qui constitue une « autorite legitime », je crois qu'il convient de clarifier cet article, et en particulier Ie terme « autorite legitime ».

Article 9

L'article 9 de la LPRPDE cause aussi certaines preoccupations aux organismes d'application de la loi, en raison d'un vide juridique qui pourrait exister dans la disposition destinee â assurer la protection des enquetes policieres. La LPRPDE prevo it que toute personne a Ie droit d'obtenir communication des renseignements

du Canada d'assurer un environnement securitaire, particulierement en matiere de transport et de transport aerien. La Loi comble certains vi des juridiques concernant Ie transport et la securite nationale en modifiant des lois existantes, telles que la *Loi sur l 'aeronautique,* Ie *Code criminel,* la *Loi sur l 'Administration canadienne de la surete du transport aerien* et d'autres lois, de meme que la LPRPDE.
Les modifications ala *Loi sur l 'aeronautique,* en particulier, visent a conferer Ie pouvoir d'exiger et d'utiliser des renseignements sur les passagers dans Ie but de proteger la securite nationale et Ie reseau acronautique canadien. Les modifications apportees aux alineas *7(l)e)* et *7(2)d)* de la LPRPDE constituent des modifications importantes, qui s'imposaient pour faire en sorte d'eviter toute incompatibilite entre les dispositions de la LPRPDE et la *Loi de 2002 sur la securite publique.*

II convient de souligner egalement qu'un des objectifs importants de la *Loi de 2002 sur la securite publique* consiste a assurer un equilibre entre l'interet de la securite publique et la protection des renseignements personnels des particuliers. La Loi comporte une serie de garanties qui visent a permettre d'atteindre cet objectiftout en assurant la transparence et la responsabilisation. Les propositions font l'objet de vastes consultations et d'un long examen au Parlement. Tout au long de ce processus, de nombreux changements ont ete effectues pour repondre aux commentaires et aux preoccupations exposes par divers intervenants, dont Ie Commissariat a la protection de la vie privee du Canada. De ce fait, les modifications ala LPRPDE figurant a l'article 98 de la *Loi de 2002 sur la securite publique* sont de portee restreinte et visent la collecte de renseignements pour les seuls besoins de satisfaire aux exigences de la loi.

Compte tenu de ce qui precede, je suis preoccupe des repercussions que pourraient avoir les changements proposes par les temoins, aux modifications deja apportees ala LPRPDE, edicte en raison de l'adoption de la *Loi de 2002 sur la securite publique,* sur l'atteinte des objectifs de la *Loi de 2002 sur la securite publique,* et pas consequent, sur la securite publique.

D'autres lois, comme les lois sur la police et Ie *Code criminel,* comportent de solides garanties a l'egard des activites d'application de la loi, de fayon a permettre un contr6le des mesures policieres de collecte et d'utilisation des renseignements personnels. En outre, les tribunaux surveillent les resultats du travail policier et s' assurent, en appliquant Ie droit de la preuve et la *Charte des droits et libertes,* que la collecte de renseignements de la police a ete faite en concordance avec les regles.

Comme vous savez, la LPRPDE a ete adoptee pour proteger les renseignements personnels en la possession des entreprises privees. Cette loi n'ajamais eu pour

Minister of Public Safety
and Emergency Preparedness

Ministre de la Securite publique
et de la Protection civile

Ottawa, Canada K1 A OP8

9 AVR 2007

Monsieur Tom Wappel, depute
President
Comite permanent de l'acces à l'information, de
la protection des renseignements personnels et
de l'ethique
Chambre des communes
Ottawa (Ontario) KIA OA6

Objet: Examen de la Loi sur la protection des renseignements personnels et les documents electroniques (LPRPDE)

Monsieur,

Je vous remercie de votre lettre du 20 mars 2007. Je suis heureux d'avoir l'occasion de contribuer aux importants travaux du Comite permanent de l'acces à l'information, de la protection des renseignements personnels et de l'ethique, de la Chambre des communes, relativement à I' examen de la *Loi sur la protection des renseignements personnels et les documents electroniques* (LPRPDE).

Vous m'avez invite à vous faire part de mon opinion concernant l'alinea *7(l)e)* de la LPRPDE, une disposition qui a ete ajoutee par l'entremise de la *Loi de 2002 sur la securite publique* ..

L'alinea 7(3)c.l) dispose qu'une organisation peut recueillir des renseignements personnels à l'insu de l'interesse et sans son consentement si la cueillette est faite aux fins de divulgation exigee par la loi ou de divulgation au gouvernement, dans les cas ou les renseignements touchent la securite nationale, la defense du Canada ou la conduite des affaires internationales, soit parce qu'ils ont ete demandes par une institution gouvernementale qui a l'autorite legitime pour les obtenir, soit de la propre initiative de I' organisation.

L'un des buts de l'alinea *7(1)e),* enchasse dans la *Loi de 2002 sur la securite publique* (qui a re9u Ia sanction royale Ie 6 mai 2004), est d'ameliorer la capacite

Canada

3.0 Moment mal choisi

Le réexamen de l'alinéa 7(1)(e) par la majorité est prématuré. Cet alinéa a été adopté dans le cadre de la *Loi sur la sécurité publique*, 2002 (2004, c. 15) et n'est entré en vigueur qu'en mai 2004. En fait, l'alinéa 7(1)(e) n'est pas couvert par cet examen législatif. En prescrivant un examen quinquennal, les rédacteurs de la LPRPDE ont déterminé qu'il serait utile pour les intervenants de profiter de cinq (5) années d'expérience avant de réfléchir à l'efficacité de la législation. L'alinéa 7(1)(e) ne faisait pas partie de la législation originale et les intervenants visés n'ont pas profité de cinq (5) années d'expérience.

4.0 Rien n'a été présenté au Comité par les intervenants

La *Loi sur la sécurité publique* a résulté d'une tentative visant à trouver un juste équilibre entre la sécurité publique et la protection des renseignements personnels. Par contre, le rapport de la majorité recommande l'abrogation d'une partie de la *Loi sur la sécurité publique* sans faire appel à la contribution des intervenants touchés, notamment les transporteurs aériens, les aéroports, les groupes de passagers aériens ou les agences de sécurité. La recommandation 14 et les paragraphes 79-85 du rapport de la majorité ne tiennent pas du tout compte du point de vue des intervenants les plus touchés par la recommandation.

Les membres du Comité appartenant au Parti conservateur notent que malgré les commentaires inclus dans le rapport de la majorité, l'honorable Stockwell Day, ministre de la Sécurité publique et de la Protection civile, a répondu au Comité, dans une lettre datée du 19 avril 2007. Les membres du Comité appartenant au Parti conservateur apprécient la contribution du ministre en rapport avec l'alinéa 7(1)(e) et l'article 9. Les membres du Comité appartenant au Parti conservateur se réjouissent que le ministre souhaite préciser le sous-alinéa 7(3)(c.1). La lettre du ministre Day est jointe en annexe à la présente opinion dissidente.

5.0 Conclusion

Les membres du Parti conservateur se dissocient énergiquement de la recommandation de la majorité parce qu'elle affaiblit les lois sur la sécurité nationale du Canada, d'autant plus que cette recommandation n'a pas profité de la contribution ni de la représentation du domaine de la sécurité ou du transport aérien.

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (le «Comité»)

Examen, prévu par la loi, de la Loi sur la protection des renseignements personnels et les documents électroniques (2000, c.5) («LPRPDE»)

OPINION DISSIDENTE

Les membres du Comité qui appartiennent au Parti conservateur souhaitent exprimer leur reconnaissance aux personnes et groupes qui ont participé en grand nombre, de manière réfléchie, à titre de témoins, et à ceux qui ont présenté des mémoires pendant l'examen. Leur contribution a été très appréciée. Pendant le processus, les membres du Parti conservateur ont découvert les réalités pratiques de la législation de la protection des renseignements personnels dans le secteur privé.

1.0 À l'écoute des petites entreprises

Comme l'indique le rapport de la majorité, la LPRPDE n'est entrée pleinement en vigueur que le 1er janvier 2004. Les membres du Parti conservateur souhaitent insister sur le fait que le rapport de la majorité vise principalement à préciser la LPRPDE plutôt qu'à prescrire des changements majeurs. Le milieu des affaires, les intervenants et les représentants officiels, notamment ceux du Commissariat à la protection de la vie privée du Canada, facilitent l'adoption de la LPRPDE. Les membres du Parti conservateur sont contre une augmentation indue du fardeau de la conformité pour les petites entreprises, qui découlerait par exemple de changements rendant la LPRPDE inutilement prescriptive. Les membres du Parti conservateur saluent les groupes, notamment la Fédération canadienne de l'entreprise indépendante, qui aident les petites et moyennes entreprises à se conformer à la LPRPDE.

2.0 Dissidence

Les membres du Parti conservateur se dissocient respectueusement de la recommandation 14 du rapport de la majorité et des motifs donnés dans les paragraphes 79 à 85 du rapport de la majorité.

L'alinéa 7(1)(e) permet à des organisations de collecter et d'utiliser de l'information en rapport avec la sécurité nationale, la défense ou les affaires internationales. Le gouvernement de l'époque avait inclus cet alinéa dans la LPRPDE expressément pour combler les lacunes législatives en rapport avec le transport et la sécurité nationale, plus particulièrement en rapport avec le transport aérien. Les membres du Comité qui appartiennent au Parti conservateur sont d'avis que l'élimination de l'alinéa 7(1)(e) pourrait menacer la sécurité du système canadien d'aviation civile.

Organisations et individus
Employeurs des transports et communications de régie fédérale (ETCOF)
Fédération des ordres des médecins du Canada
Gendarmerie royale du Canada
IMS Health Canada
Inforoute Santé du Canada
Kerr, Ian
Law Society of Alberta
Ministère des Services gouvernementaux
Mouvement des caisses Desjardins
Murray Long & Associés
National Association for Information Destruction – Canada
Speers, Richard

ANNEXE B
LISTE DES MÉMOIRES

Organisations et individus

Advocis

Association canadienne de la technologie de l'information

Association canadienne de la technologie de l'information

Association canadienne de l'immeuble

Association canadienne des compagnies d'assurances de personnes inc.

Association canadienne des courtiers de fonds mutuels

Association canadienne du marketing

Association dentaire canadienne

Association des banquiers canadiens

Association du Barreau canadien

Association of Canadian Archivists

B.C. Freedom of Information and Privacy Association (FIPA)

Burbidge, Scott

Bureau d'assurance du Canada

Bureau d'assurance du Canada

Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique

Centrale des caisses de crédit du Canada

Centre canadien de ressources pour les victimes de crimes

Centre pour la défense de l'intérêt public

Chambre de commerce du Canada

Clinique d'intérêt public et de politique d'Internet du Canada

Commissariat à la protection de la vie privée du Canada

Gendarmerie royale du Canada Art Crockett, officier responsable, Services stratégiques, Opérations techniques	2007/02/20	32
Gendarmerie royale du Canada Earla-Kim McColl, surintendante, Centre national de coordination contre l'exploitation des enfants	2007/02/20	32
Commissariat à la protection de la vie privée du Canada Jennifer Stoddart, commissaire à la protection de la vie privée	2007/02/22	33
Commissariat à la protection de la vie privée du Canada Heather Black, commissaire adjointe (LPRPDÉ)	2007/02/22	33

Centrale des caisses de crédit du Canada Charlene Loui-Ying, avocate générale et agente des relations gouvernementales Credit Union Central of British Columbia	2007/01/30	26
Association canadienne des compagnies d'assurances de personnes inc. Yves Millette, vice-président en chef, Affaires du Québec	2007/02/01	27
Association canadienne des compagnies d'assurances de personnes inc. Dale Philp, vice-président adjoint et avocat principal , Financière Sun Life	2007/02/01	27
Association canadienne des compagnies d'assurances de personnes inc. Frank Zinatelli, vice-président et co-directeur du contentieux	2007/02/01	27
Chambre de commerce du Canada David Elder, vice-président, Loi de nature réglementaire Bell Canada	2007/02/01	27
Chambre de commerce du Canada Chris Gray, analyste des politiques	2007/02/01	27
Chambre de commerce du Canada Michael Murphy, vice-président exécutif, Politiques	2007/02/01	27
Bureau d'assurance du Canada Randy Bundus, vice-président, Conseiller juridique en chef et secrétaire de la société	2007/02/06	28
Bureau d'assurance du Canada Mark Yakabuski, vice-président, Affaires fédérales et Ontario	2007/02/06	28
Dominion of Canada General Insurance Company Vivian Bercovici, avocate	2007/02/06	28
Dominion of Canada General Insurance Company Ann MacKenzie, agent de la protection de la vie privée	2007/02/06	28
Murray Long & Associés Murray Long, président	2007/02/06	28
IMS Health Canada Gary Fabian, vice-président, Affaires publiques et relations corporatives	2007/02/08	29

ANNEXE A
LISTE DES TÉMOINS

Organisations et individus	Date	Réunion
Ministère de l'Industrie Michael Binder, sous-ministre adjoint, Spectre, technologies de l'information et télécommunications	2006/11/20	17
Ministère de l'Industrie Danièle Chatelois, analyste de la politique sur la vie privée, Direction de la politique sur le commerce électronique, Direction générale sur le commerce électronique	2006/11/20	17
Ministère de l'Industrie Richard Simpson, directeur générale, Commerce éléctronique	2006/11/20	17
Ministère de la Justice Alexia Taschereau, avocate - conseil, Industrie Canada	2006/11/20	17
À titre personnel Colin Bennett, professeur de science politique, Université de Victoria	2006/11/22	18
B.C. Freedom of Information and Privacy Association (FIPA) Richard Rosenberg, président	2006/11/22	18
Commissariat à la protection de la vie privée du Canada Jennifer Stoddart, commissaire à la protection de la vie privée	2006/11/27	19
Commissariat à la protection de la vie privée du Canada Heather Black, commissaire adjointe (LPRPDÉ)	2006/11/27	19
Commissariat à la protection de la vie privée du Canada Melanie Millar-Chapman, analyste de recherche stratégique et politique	2006/11/27	19
À titre personnel Valerie Steeves, Département de criminologie, Université d'Ottawa	2006/11/29	20
Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique David Loukidelis, commissaire	2006/11/29	20

DEMANDE DE RÉPONSE DU GOUVERNEMENT

Conformément à l'article 109 du *Règlement*, le Comité demande au gouvernement de déposer une réponse globale au présent rapport.

Respectueusement soumis,

Le président

Tom Wappel, député

Recommandation 23

Le Comité recommande que la LPRPDE soit modifiée par l'ajout d'une disposition obligeant les organisations à signaler certaines violations précises de la confidentialité de leurs fonds de renseignements personnels à la commissaire à la protection de la vie privée.

Recommandation 24

Le Comité recommande que, dès qu'une organisation lui signale une atteinte à la confidentialité de son fonds de renseignements personnels, la commissaire à la protection de la vie privée décide s'il y a lieu ou non d'en informer les personnes concernées ainsi que d'autres personnes et, dans l'affirmative, détermine la façon de procéder à cette fin.

Recommandation 25

Le Comité recommande qu'au moment de décider des détails d'un modèle d'avis adapté à la LPRPDE, il faudra aussi prendre en considération le moment et la façon de signaler les atteintes, les sanctions en cas de défaut d'aviser, et la nécessité de prévoir un pouvoir d'aviser « sans consentement » les agences d'évaluation du crédit afin d'aider à protéger les consommateurs contre le vol d'identité et la fraude.

Recommandation 19

Le Comité recommande qu'aucune modification ne soit apportée au paragraphe 20(2) de la LPRPDE en ce qui concerne le pouvoir discrétionnaire de la commissaire à la protection de la vie privée de divulguer l'identité d'une organisation dans l'intérêt public.

Recommandation 20

Le Comité recommande qu'en vertu de la LPRPDE, la commissaire fédérale à la protection de la vie privée soit habilitée à partager des renseignements personnels et à coopérer, dans le cadre d'enquêtes d'intérêt mutuel, avec ses homologues des provinces où il n'y a pas de lois essentiellement similaires à la loi fédérale pour le secteur privé, ainsi qu'avec les instances responsables de la protection des données à l'étranger.

Recommandation 21

Le Comité recommande que les renseignements partagés avec d'autres pays, particulièrement les États-Unis, soient dûment protégés de façon à ne pas être divulgués à un tribunal étranger ou à une autre instance gouvernementale à des fins autres que celles pour lesquelles ils ont été communiqués.

Recommandation 22

Le Comité recommande que la LPRPDE soit modifiée afin que la commissaire à la protection de la vie privée soit habilitée à demander à la Cour fédérale du Canada un examen accéléré d'une allégation de secret professionnel liant un avocat à son client invoquée pour refuser l'accès à des renseignements personnels (alinéa 9(3)*a*)), lorsque la commissaire s'est fait refuser la production d'information dans le cadre d'une enquête.

Recommandation 13

Le Comité recommande que l'expression « institution gouvernementale » aux alinéas 7(3)*c*.1) et *d*) de la LPRPDE soit éclaircie afin de préciser si elle comprend les entités municipales, provinciales, territoriales, fédérales et non canadiennes.

Recommandation 14

Le Comité recommande que l'alinéa 7(1)*e*) soit retiré de la LPRPDE.

Recommandation 15

Le Comité recommande que le gouvernement examine la question du consentement des mineurs concernant la collecte, l'utilisation et la communication de leurs renseignements personnels dans un contexte commercial, en vue de modifier la LPRPDE à cet égard.

Recommandation 16

Le Comité recommande que le gouvernement examine la question du consentement des mineurs concernant la collecte, l'utilisation et la communication de leurs renseignements personnels dans un contexte commercial, en vue de modifier la LPRPDE à cet égard.

Recommandation 17

Le Comité recommande que le gouvernement consulte les membres du secteur des soins de santé et le Commissariat à la protection de la vie privée du Canada afin de déterminer quels éléments du document sur les outils de sensibilisation à la LPRPDE pourraient être énoncés sous forme législative.

Recommandation 18

Le Comité recommande qu'aucun pouvoir de rendre des ordonnances ne soit octroyé pour l'instant à la commissaire fédérale à la protection de la vie privée.

LISTE DES RECOMMANDATIONS

Recommandation 1

Le Comité recommande qu'une définition des coordonnées des entreprises soit ajoutée à la LPRPDE et que soient prises en considération, à cette fin, la définition et la disposition limitative connexe qui se trouvent dans la Loi sur la protection des renseignements personnels de l'Alberta.

Recommandation 2

Le Comité recommande que la LPRPDE soit modifiée pour y inclure une définition du « produit du travail » qui précise explicitement que ce dernier ne constitue pas des renseignements personnels aux fins de la Loi. La définition devrait s'inspirer de la définition des « renseignements sur le produit du travail » contenue dans la Loi sur la protection des renseignements personnels de la Colombie-Britannique, de la définition proposée au Comité par IMS Canada et de l'approche adoptée au Québec dans la *Loi sur la protection des renseignements personnels dans le secteur privé* à l'égard des renseignements personnels de professionnels.

Recommandation 3

Le Comité recommande qu'une définition de « destruction » soit ajoutée à la LPRPDE afin de guider les organisations sur la façon de bien détruire les documents papier et les fichiers électroniques.

Recommandation 4

Le Comité recommande d'envisager de modifier la LPRPDE pour y préciser les exigences applicables à la forme et à la conformité du consentement et établir une distinction entre les différentes formes de consentement : explicite, implicite et présumé/refusé. Il conviendrait, à cet égard, de se reporter aux Lois de l'Alberta et de la Colombie-Britannique en matière de protection des renseignements personnels.

Recommandation 25

Le Comité recommande qu'au moment de décider des détails d'un modèle d'avis adapté à la LPRPDE, il faudra aussi prendre en considération le moment et la façon de signaler les atteintes, les sanctions en cas de défaut d'aviser, et la nécessité de prévoir un pouvoir d'aviser « sans consentement » les agences d'évaluation du crédit afin d'aider à protéger les consommateurs contre le vol d'identité et la fraude.

Le Comité reconnaît que la question du niveau de gravité intervient dans deux aspects du modèle qu'il recommande : 1) pour déterminer les situations où une organisation doit signaler une atteinte à la sécurité des données à la commissaire à la protection de la vie privée; 2) pour permettre à la commissaire de décider si l'atteinte doit être signalée ou non. Dans le premier cas, nous souhaitons éviter d'ensevelir la commissaire sous les avis d'atteinte. En exigeant que le Commissariat à la protection de la vie privée soit avisé de toutes les atteintes à la sécurité, on risque de lui imposer un fardeau excessif qui aura, à tout le moins, des répercussions importantes sur le plan des ressources. Nous sommes d'avis que cet aspect doit être soigneusement pris en considération avant d'ajouter à la LPRPDE une disposition législative sur les atteintes à signaler.

Le Comité n'est donc pas d'accord avec ce que certains appellent « l'obligation de donner avis d'une atteinte », soit le fait d'aviser toute personne dont les renseignements personnels ont été compromis, chaque fois qu'il y a une atteinte. Nous proposons que les organisations informent la commissaire à la protection de l'information de certaines atteintes à la sécurité bien définies, afin que son bureau puisse aider à déterminer s'il faut aviser les personnes visées et, le cas échéant, de quelle manière. La commissaire exercerait un pouvoir discrétionnaire en cette deuxième étape du processus, puisqu'elle déciderait au cas par cas s'il doit y avoir un avis.

Le Comité estime qu'en ce qui concerne les détails d'un modèle adapté à la LPRPDE, il faudra se pencher sur les questions de niveau de gravité, par exemple les cas où il faudra signaler à la commissaire à la protection de la vie privée les atteintes aux fonds de renseignements personnels, ainsi que les cas où la commissaire exigera qu'avis soit donné des atteintes signalées. Il faudra également prendre en compte le moment et la façon de donner avis, les sanctions en cas de défaut d'aviser, et la nécessité de prévoir un pouvoir d'aviser « sans consentement » les agences d'évaluation du crédit afin d'aider à protéger les consommateurs contre le vol d'identité et la fraude.

Recommandation 23

Le Comité recommande que la LPRPDE soit modifiée par l'ajout d'une disposition obligeant les organisations à signaler certaines violations précises de la confidentialité de leurs fonds de renseignements personnels à la commissaire à la protection de la vie privée.

Recommandation 24

Le Comité recommande que, dès qu'une organisation lui signale une atteinte à la confidentialité de son fonds de renseignements personnels, la commissaire à la protection de la vie privée décide s'il y a lieu ou non d'en informer les personnes concernées ainsi que d'autres personnes et, dans l'affirmative, détermine la façon de procéder à cette fin.

approprié et signale que l'obligation d'aviser ne s'inscrit pas facilement dans le modèle de la LPRPDE puisqu'il n'existe pas de moyen de sanctionner directement les organisations en cas de défaut d'aviser les particuliers des atteintes à la sécurité. La commissaire a toutefois recommandé comme ajout ou comme solution de rechange à l'obligation d'aviser, l'adjonction à la LPRPDE d'une disposition qui habiliterait une organisation dont la sécurité a été violée à informer les agences d'évaluation du crédit de cette violation et des personnes touchées, sans avoir à obtenir le consentement de ces dernières. Les agences pourraient ainsi se montrer plus proactives dans la protection des consommateurs contre le vol d'identité et la fraude.

Cependant, lors de sa dernière comparution devant le Comité, la commissaire à la protection de la vie privée a signalé que plusieurs fuites importantes qui se sont produites récemment ont accru l'urgence de résoudre la question; par conséquent, elle recommande maintenant de modifier la LPRPDE en y ajoutant une disposition touchant les avis d'atteinte à la sécurité des renseignements personnels. En attendant que cette modification soit apportée, la commissaire continuera de travailler en collaboration avec les parties prenantes à l'élaboration de lignes directrices facultatives. Lorsque les membres du Comité l'ont interrogée au sujet de sa position sur la question, la commissaire a répondu qu'à son avis, l'introduction d'une modification à la LPRPDE n'aurait pas de grande incidence sur les pratiques actuelles des organisations lors d'atteinte à la sécurité des données.

Le Comité estime qu'il faut modifier la LPRPDE afin d'inclure une disposition exigeant que les atteintes à la sécurité des renseignements personnels soient signalées; cependant, nous reconnaissons que ce ne sera pas tâche facile. Nous préconisons un modèle en vertu duquel les organisations seraient tenues de signaler les atteintes à la commissaire à la protection de la vie privée, qui effectuerait ensuite une analyse pour déterminer s'il faut ou non donner avis. Mais un élément est essentiel à l'élaboration d'un modèle législatif, soit la détermination du niveau de gravité de l'atteinte.

Le Comité a entendu des témoignages à l'effet qu'il faudrait établir une sorte de norme en matière d'avis qui tiendrait compte de la nature et l'ampleur de l'atteinte. La CIPPIC, par exemple, prône le modèle législatif adopté en Californie qui énonce qu'il y a devoir de signaler une atteinte seulement s'il y a acquisition de renseignements personnels par une personne non autorisée ou s'il existe un motif raisonnable de croire à une acquisition de ce genre. Une telle norme est perçue comme étant plus sévère que le simple accès par une personne non autorisée, mais aussi moins stricte que le risque de vol d'identité. L'Association du Barreau canadien recommande une exigence équilibrée en matière d'avis, soit l'obligation d'aviser uniquement lorsque l'organisation n'est pas dotée de mécanismes de sécurité (par exemple le cryptage ou la dépersonnalisation) ou lorsqu'elle a reçu un avis que ces mécanismes ont été violés et que les renseignements mis en cause sont de nature délicate.

La Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) a publiés un livre blanc sur les avis d'atteinte à la sécurité des renseignements personnel[33], qui formule des recommandations précises en vue d'une modification de la LPRPDE. Elle demande dans ce document que les lois canadiennes obligent les organisations à aviser les personnes dont les renseignements personnels ont été compromis par suite d'une atteinte à leur sécurité. Elle réclame en particulier de modifier la LPRPDE afin d'exiger que les atteintes à la sécurité soient signalées si certains types de renseignements personnels sont exposés à un accès non autorisé. Le livre blanc analyse et appuie parfois certains aspects des dispositions législatives américaines sur les atteintes à la sécurité; plus de la moitié des États américains se dont d'ailleurs dotés d'une obligation de signaler les atteintes à la sécurité, et plusieurs lois fédérales sont à l'étude.

Murray Long, spécialiste de la protection de la vie privée, a aussi fourni au Comité un projet en quatre points concernant l'avis d'atteinte à la sécurité des renseignements personnels. En premier lieu, il devrait être obligatoire de signaler les atteintes à la sécurité de tous les types d'information sensible, pas seulement des données financières. Deuxièmement, la décision d'aviser la population devrait être laissée à la discrétion des organisations, mais celles-ci devraient décider en fonction d'une autoévaluation et d'une norme objective afin d'agir avec prudence. La norme objective exigerait qu'une organisation informe la commissaire à la protection de la vie privée lorsqu'une personne raisonnable pourrait considérer qu'il convient de le faire, dans un court délai prescrit par la loi. Troisièmement, l'organisation serait alors tenue de décrire à la commissaire l'impact de l'atteinte, les efforts déployés pour atténuer les conséquences et la décision prise pour ce qui est d'aviser les personnes visées. L'organisation qui décide de ne pas aviser les intéressés serait tenue d'expliquer pourquoi, et la commissaire à la protection de la vie privée pourrait alors évaluer la décision. Quatrièmement, le défaut d'aviser les intéressés, quand une personne raisonnable pourrait s'attendre à ce qu'il y ait divulgation, devrait constituer une infraction aux termes de la Loi[34].

Le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, David Loukidelis, a mis en garde contre l'adoption intégrale des exigences d'avis explicite adoptées aux États-Unis, disant que rien encore ne prouve que l'obligation d'aviser constitue un moyen économique de réduire le risque de vol d'identité découlant d'atteintes à la sécurité.

Lors de sa première comparution devant le Comité, la commissaire fédérale à la protection de la vie privée s'est aussi montrée prudente dans ce dossier. Elle appuie l'idée d'une obligation d'aviser, mais elle souligne combien il est difficile de choisir un modèle

---

33 Clinique d'intérêt public et de politique d'Internet du Canada, *Approaches to Security Breach Notification: A White Paper*, 9 janvier 2007, http://www.cippic.ca/en/bulletin/BreachNotification_9jan07-web.pdf.

34 Le modèle proposé par M. Long comporte un autre élément : modifier la section de la Loi portant sur les droits des dénonciateurs afin que la notification d'atteinte donnée de bonne foi figure parmi les droits protégés des employés.

De façon générale, les représentants de l'industrie se sont montrés favorables aux directives formulées par les commissaires à la protection de la vie privée du Canada, de la Colombie-Britannique et de l'Ontario. Les commissaires à l'information et à la protection de la vie privée de l'Ontario et de la Colombie-Britannique ont publié ensemble un outil d'évaluation intitulé *Breach Notification Assessment Tool*[32], afin d'aider les organisations à déterminer les mesures à prendre en cas d'atteinte à la vie privée. La commissaire fédérale et son bureau travaillent également en collaboration avec l'industrie afin d'élaborer à l'intention des organisations des lignes directrices d'application facultative en cas de violation de la confidentialité. Comme l'a expliqué au Comité David Elder, de la Chambre de commerce du Canada :

> La Chambre de commerce du Canada ne croit pas qu'il est nécessaire d'inscrire dans la législation l'obligation de **notifier**. Nous encourageons plutôt les entreprises à continuer de collaborer étroitement avec la commissaire à la protection de la vie privée pour repérer les cas de violation et notifier les personnes qui peuvent être affectées par une éventuelle violation de leur vie privée. Ce mécanisme souple permet de notifier au besoin, sans effet négatif sur les consommateurs. J'aimerais aussi faire remarquer qu'il serait avantageux pour la Chambre de commerce du Canada et pour d'autres associations d'entreprises d'élaborer un ensemble de lignes directrices fondées sur les pratiques exemplaires, qu'elles pourraient utiliser lorsque des violations de la vie privée surviennent. À cette fin, les groupes d'entreprises, notamment la Chambre de commerce du Canada, l'ACTI, l'ACM, etc., sont en train d'élaborer des lignes directrices pour la notification en cas de violation conjointement avec la commissaire à la protection de la vie privée. Des détails concernant ces lignes directrices seront disponibles plus tard ce printemps. (1er février 2007)

Ceux qui prônent l'ajout à la LPRPDE d'une disposition, exigeant que les atteintes soient signalées, invoquent la nécessité d'informer les consommateurs afin de leur permettre de se défendre efficacement contre l'accroissement des vols d'identité au Canada. Dans son mémoire au Comité, le Centre pour la défense de l'intérêt public présente l'explication suivante :

> La seule façon d'atteindre cet objectif consiste à imposer à chaque organisation l'obligation de signaler au CPVPC toute atteinte à la sécurité des données et d'informer toutes les personnes dont les renseignements personnels ont été ainsi compromis. De plus, cette obligation ne devrait pas être diluée ou faire l'objet de restrictions. L'organisation chargée de préserver et de protéger des renseignements personnels devrait être tenue d'informer la personne concernée chaque fois qu'il y a atteinte à la sécurité des renseignements en question. Ainsi, chaque personne serait en mesure de prendre ses propres décisions sur les prochaines mesures à prendre. Ce n'est pas l'organisation qui devrait déterminer unilatéralement le degré de risque associé au manquement ou la gravité du préjudice possible. (23 octobre 2006, p. 19)

---

[32] Commissaires à l'information et à la protection de la vie privée de la Colombie-Britannique et de l'Ontario, *Breach Notification Assessment Tool*, décembre 2006, http://www.ipc.on.ca/images/Resources/up-ipc_bc_breach.pdf.

AVIS D'ATTEINTE À LA SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS

La plupart des témoins ont abordé la question du devoir des organisations d'aviser les particuliers dans les cas d'atteinte à la sécurité des fonds de renseignements personnels. À l'heure actuelle, il n'y a aucune obligation à cet égard, bien que le Comité ait été informé que, dans la pratique, les organisations consultent souvent le Commissariat à la protection de la vie privée afin de savoir si elles doivent aviser leurs clients d'une violation et, le cas échéant, comment elles doivent s'y prendre. Les entreprises réagissent donc, chacune à leur manière, aux fuites de renseignements, en tenant compte de facteurs comme le nombre de personnes touchées, la nature des données visées et la possibilité que les renseignements soient utilisés à des fins répréhensibles. Ces questions suscitent de plus en plus de préoccupations à mesure que les grands quotidiens font état d'un nombre croissant de fuites importantes de renseignements personnels touchant de nombreux Canadiens.

De nombreux États américains ont adopté des mesures législatives exigeant que les clients soient informés quand la confidentialité de leurs renseignements personnels est compromise. La plupart de ces lois prévoient d'importantes amendes en cas d'omission de notification. Au Canada, seule la *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario oblige à donner avis en cas d'atteinte à la confidentialité. La Loi exige que les dépositaires de renseignements sur la santé avisent à la première occasion raisonnable les particuliers concernés s'il y a vol ou perte de renseignements ou si des personnes non autorisées y ont accès[31].

La plupart des entreprises estiment déjà être tenues d'aviser les particuliers s'il y a d'importantes fuites de renseignements personnels. Soulignant que le principe de transparence (principe 8) du code type de CSA sur la protection des renseignements personnels, qui figure à l'annexe 1 de la LPRPDE, laisse déjà entendre que les organisations ont des responsabilités à cet égard, elles jugent pour l'instant inutile d'adopter des dispositions législatives particulières. L'Association canadienne des compagnies d'assurances de personnes inc. a décrit son approche axée sur l'autoévaluation et le risque :

> L'industrie prône, en matière de **notification**, une approche axée sur le risque, où la nécessité d'aviser et la méthode employée pour informer le particulier sont proportionnelles au risque de préjudice que pourraient vivre les personnes dont les renseignements personnels ont été compromis. Selon une telle approche, il est nécessaire d'aviser l'intéressé si : la violation est substantielle; l'organisation a des motifs raisonnables de croire que des renseignements personnels ont été communiqués à des personnes non autorisées; la communication présente un risque considérable de porter préjudice à des individus (par exemple le vol d'identité ou la fraude). [traduction] (1er février 2007, mémoire, p. 11-12)

---

31 Paragraphe 12(21).

Vivian Bercovici, de la compagnie d'assurance générale Dominion of Canada, appuie pour sa part la décision de la Cour fédérale du Canada dans l'affaire Blood Tribe et s'élève contre la modification demandée par la commissaire à la protection de la vie privée :

> [...] le secret professionnel de l'avocat est au centre de l'ordre et de l'intégrité de notre système de justice. Une personne ou une partie à une procédure doit savoir avec certitude que toute communication qu'elle a avec son avocat restera confidentielle. Cela permet à l'avocat d'avoir des communications libres et exemptes de toute menace avec son client, ce qui facilite la préparation et la présentation d'une défense complète et énergique. Exprimer des réserves au sujet du secret professionnel de l'avocat, qui est ancré depuis des siècles dans la tradition de la common law, serait catastrophique. (6 février 2007)

Le Comité pense comme la commissaire qu'il faut un moyen de vérifier de façon indépendante s'il est légitime d'invoquer le secret professionnel liant un avocat à son client est appropriée pour refuser l'accès à des renseignements personnels en vertu de l'article 9 de la LPRPDE. Cependant, nous ne croyons pas que la vérification doit être liée au processus et aux pouvoirs d'enquête du Commissariat. Nous ne sommes pas convaincus non plus que l'article 15 de la LPRPDE offre actuellement à la commissaire la latitude voulue pour pouvoir contester devant la Cour fédérale une allégation selon laquelle des renseignements sont protégés par le secret professionnel, lorsqu'il lui est impossible de prendre connaissance des documents en question. Nous recommandons donc de modifier la LPRPDE de manière à habiliter le Commissariat à la protection de la vie privée à demander à un juge de la Cour fédérale d'effectuer un examen accéléré de l'allégation de secret professionnel. Si le juge détermine que le privilège du secret professionnel a été invoqué à mauvais escient, la Cour pourra ordonner à l'intéressé de produire les documents en cause.

Le Comité sait que sa recommandation donnera lieu à un mécanisme différent de celui que prévoit la *Loi sur la protection des renseignements personnels;* cependant, étant donné que la LPRPDE n'a pas la même origine ni le même objectif que la loi visant le secteur public fédéral, nous ne nous sentons pas tenus d'appliquer à la première les principes qui sous-tendent cette dernière.

Recommandation 22

Le Comité recommande que la LPRPDE soit modifiée afin que la commissaire à la protection de la vie privée soit habilitée à demander à la Cour fédérale du Canada un examen accéléré d'une allégation de secret professionnel liant un avocat à son client invoquée pour refuser l'accès à des renseignements personnels (alinéa 9(3)*a*)), lorsque la commissaire s'est fait refuser la production d'information dans le cadre d'une enquête.

privée qui doit faire enquête. Or, la commissaire à la protection de la vie privée affirme que pour exercer ce pouvoir d'enquête, elle doit avoir accès aux documents visés par le secret afin de pouvoir déterminer si la communication a été refusée à bon escient en vertu de la Loi. Elle jouit actuellement de ce pouvoir en vertu du paragraphe 34(2) de la *Loi sur la protection des renseignements personnels*, mais aucune disposition à cet effet ne figure dans la LPRPDE, car on n'avait pas cru qu'une telle omission soulèverait des difficultés. Les tribunaux se penchent actuellement sur la question.

La commissaire à la protection de la vie privée a demandé en particulier au Comité de se pencher sur la récente décision de la Cour fédérale du Canada dans l'affaire *Blood Tribe*[30], qui pourrait permettre à une organisation d'invoquer le secret professionnel liant un avocat à son client pour empêcher le Commissariat d'examiner des documents lors d'une enquête. Cette décision dépouillera le Commissariat du pouvoir d'exiger la production de documents afin de les examiner et de vérifier s'ils contiennent vraiment des renseignements protégés par le secret professionnel. La commissaire exprime ainsi ses préoccupations :

> Je voudrais parler d'une question très précise et urgente concernant une décision récente de la Cour fédérale du Canada. L'affaire porte sur le secret professionnel qui lie un avocat à son client et notre capacité d'avoir accès à des documents. La récente décision rendue dans l'affaire Blood Tribe crée une lacune béante dans notre capacité de mener des enquêtes dignes de ce nom. Elle permet ainsi aux organisations de refuser à nos enquêteurs l'accès à des renseignements personnels, sans vérification indépendante du fait que les documents visés contiennent bien des renseignements assujettis au secret professionnel. Bien que nous demandions l'autorisation d'interjeter appel de la décision, nous croyons qu'il faut dissiper cette ambiguïté en modifiant le plus rapidement possible la LPRPDE. (27 novembre 2006)

Dans l'affaire Blood Tribe, la Cour fédérale du Canada s'est penchée sur le pouvoir du Commissariat d'exiger la production de documents qui seraient protégés par le secret professionnel et a jugé que le Parlement, lorsqu'il a adopté la LPRPDE, n'avait pas l'intention de conférer au Commissariat des pouvoirs d'enquête absolus. Selon la Cour, il faut une indication explicite dans la Loi pour pouvoir passer outre au privilège du secret professionnel, à défaut de quoi, le Commissariat n'est pas habilité à exiger la production de documents afin de vérifier la légitimité du privilège. La Cour souligne que dans les cas où on invoque de façon générale le secret professionnel pour faire échec à une enquête, la commissaire peut, en vertu de l'article 15 de la LPRPDE, s'adresser à la Cour fédérale afin de demander qu'un juge examine l'allégation de secret professionnel.

---

30 *Blood Tribe Department of Health c. Canada (commissaire à la protection de la vie privée du Canada)* 2006 CAF 334, Cour d'appel fédérale, infirmant *Blood Tribe Department of Health c. Canada (commissaire à la protection de la vie privée)*(C.F.) 2005 4 R.C.F. 34.

> pratique obligatoire visant à identifier les défendeurs nuirait dans tous les cas aux parties dans le cadre d'un litige, en plus de donner lieu à de fâcheuses conséquences. Le règlement d'une plainte se traduit souvent par un changement de politique et de procédure de la part de la société visée, de sorte que tous les consommateurs en bénéficient au bout du compte. Ainsi, il est possible d'obtenir des résultats positifs, et ce, d'une manière hautement efficace. (11 décembre 2006)

La commissaire n'a pas présenté de recommandations détaillées au Comité à ce sujet, mais elle a fourni un article qui résume sa position[28]. Elle insiste sur la nécessité de la confidentialité dans le cadre du modèle de l'ombudsman puisqu'il encourage les plaignants à être plus ouverts au risque de se rendre vulnérables, tout en permettant aux défendeurs d'être plus critiques face à eux-mêmes et d'accepter de modifier leurs pratiques. Cela dit, la commissaire admet que la Loi prévoit une exception à la règle de la confidentialité lorsqu'il est dans l'intérêt du public de divulguer le nom d'un défendeur. L'exception étant circonscrite, un certain nombre de critères sont censés régir son application. Par exemple, la décision de divulguer un nom doit être prise au cas par cas, le motif de la divulgation et la raison pour laquelle le pouvoir discrétionnaire est accordé doivent être rationnellement liés, et seuls doivent être rendus publics les renseignements nécessaires aux fins recherchées.

En grande partie pour les mêmes raisons que celles invoquées concernant le pouvoir de rendre des ordonnances, le Comité estime qu'il serait prématuré de modifier le pouvoir du Commissariat de divulguer l'identité des contrevenants. Le Comité appuie l'usage que fait la commissaire de ses pouvoirs discrétionnaires en vertu du paragraphe 20(2) et recommande qu'aucun changement ne soit apporté à la Loi à cet égard.

Recommandation 19

Le Comité recommande qu'aucune modification ne soit apportée au paragraphe 20(2) de la LPRPDE en ce qui concerne le pouvoir discrétionnaire de la commissaire à la protection de la vie privée de divulguer l'identité d'une organisation dans l'intérêt public.

3. Partage d'information avec d'autres autorités responsables de données

Comme nous l'avons souligné pour la divulgation de l'identité d'un contrevenant, le Commissariat à la protection de la vie privée doit généralement considérer confidentiel tout renseignement obtenu dans l'exercice de ses attributions. En d'autres mots, le Commissariat n'a pas le droit, sauf dans certains cas très précis, de communiquer des renseignements au sujet d'un plaignant sans le consentement de ce dernier. L'article 23 de

---

[28] Jennifer Stoddart, « Cherry Picking Among Apples and Oranges: Refocusing Current Debate About the Merits of the Ombuds-Model under PIPEDA », *Canadian Business Law Journal*, volume 44, n° 1, p. 9-12.

2. Divulgation de l'identité des contrevenants

À l'heure actuelle, le paragraphe 20(1) de la LPRPDE stipule que la commissaire et les personnes agissant en son nom ou sous son autorité sont tenues au secret en ce qui concerne les renseignements dont ils prennent connaissance dans l'exercice des attributions que leur confère la Loi. Cependant, le paragraphe 20(2) autorise la commissaire à rendre publique toute information relative aux pratiques d'une organisation en matière de gestion des renseignements personnels, si elle estime que cela est dans l'intérêt public. C'est sur ce cas d'exception circonscrit qu'ont porté les témoignages recueillis par le Comité.

De nombreux partisans de la protection de la vie privée ont exhorté le Comité à modifier la LPRPDE afin d'obliger la commissaire à rendre public le nom de toutes les organisations qui contreviennent à la Loi. D'aucuns ont fait valoir, par exemple, que les organisations devraient être responsables de leurs actions devant le public et que, en l'absence d'un pouvoir de rendre des ordonnances pour faire respecter la Loi, le public doit pouvoir exiger que les contrevenants rendent des comptes. Philippa Lawson, de la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC), a présenté les arguments suivants :

> La commissaire à la protection de la vie privée hésite trop à utiliser les pouvoirs dont elle dispose. Parmi ces pouvoirs, le plus important est celui de divulguer toute information obtenue dans le cadre de ses enquêtes, si c'est dans l'intérêt public de le faire. Ce pouvoir est prévu au paragraphe 20(2). La commissaire a indiqué qu'elle ne l'utilisera jamais. Sauf, peut-être, dans le cas de récidivistes. [...] Cependant, pour que les consommateurs puissent exercer une pression sur les entreprises délinquantes en matière de protection de la vie privée, ils doivent pouvoir exprimer leur mécontentement de ces entreprises. Cela n'est pas possible lorsque l'entreprise est protégée de toute mauvaise publicité et de tout recours par les consommateurs. Si vous ne recommandez pas qu'on donne à la commissaire plein pouvoir d'ordonnance nous vous demandons à tout le moins de demander que l'article 20 de la LPRPDE soit modifié pour exiger la publication du nom des entreprises délinquantes. (6 décembre 2006)

Par contre, les organisations estiment que l'exercice du pouvoir du Commissariat à cet égard doit rester discrétionnaire. Le fait de nommer une organisation chaque fois que le Commissariat constate un non-respect de la Loi pourrait être préjudiciable à la réputation de l'entreprise et même induire le consommateur en erreur (par exemple lorsqu'une erreur mineure a été corrigée sans que le consommateur ne subisse de préjudice ou lorsque le dossier concerne une seule division d'une grande entreprise). Ariane Siegel, de l'Association canadienne de la technologie de l'information (ACTI), a formulé les observations suivantes :

> Actuellement, il est fait état de la plupart des résumés sous le couvert de l'anonymat. La commissaire a adopté la position selon laquelle le fait de nommer les défendeurs ne correspond pas dans tous les cas à l'objectif d'intérêt public de la législation. L'ACTI approuve cette approche. La commissaire peut toutefois utiliser le pouvoir discrétionnaire qui lui est conféré pour nommer les défendeurs. L'ACTI est d'avis que l'adoption d'une

La commissaire fédérale à la protection de la vie privée, pour sa part, a clairement indiqué qu'elle ne voit pas la nécessité de modifier ses pouvoirs pour l'instant;

> Je crois que cette question devrait être réglée à un moment plus opportun. Au cours des trois dernières années et demie, le Commissariat a tenté d'effectuer son travail avec une capacité administrative restreinte et dans une atmosphère d'instabilité et de surveillance de tous les instants. Nous émergeons tout juste de cette difficile étape. Nous voici réorganisés, renouvelés, et on nous a promis des ressources suffisantes. À notre avis, l'octroi du pouvoir de rendre des ordonnances aurait, pour l'instant, des conséquences administratives qui nous empêcheraient de satisfaire à un mandat aux multiples facettes (27 novembre 2006, mémoire)

De plus, la commissaire affirme que la Loi n'est pas en vigueur depuis assez longtemps pour lui avoir permis d'exercer tous les pouvoirs d'exécution qu'elle lui confère. Ainsi, la commissaire n'a pas encore eu l'occasion de s'adresser à la Cour fédérale pour réclamer des dommages, l'étendue de ses pouvoirs de vérification n'a pas encore été déterminée et certaines des dispositions pénales prévues dans la Loi n'ont pas encore été appliquées.

Compte tenu des préoccupations soulevées par la commissaire fédérale à la protection de la vie privée, le Comité estime qu'il est trop tôt pour modifier les pouvoirs d'exécution que prévoit la Loi. Le modèle de l'ombudsman nous paraît convenir pour obtenir qu'une organisation faisant l'objet d'une plainte se conforme à la Loi. De plus, nous pensons, comme la commissaire, qu'il est prématuré d'envisager d'ajouter un pouvoir de rendre des ordonnances avant qu'elle ait eu l'occasion d'explorer pleinement les pouvoirs d'exécution et d'utiliser davantage tous les pouvoirs que la Loi lui confère.

Le Comité reconnaît qu'il faudra peut-être, un jour, recommander que le pouvoir de rendre des ordonnances soit octroyé à la commissaire, s'il s'avère que les pouvoirs actuels de cette dernière ne lui permette pas de faire dûment respecter et observer la Loi. De plus, le Comité est bien conscient que tout changement apporté aux pouvoirs du Commissariat à la protection de la vie privée doit être étudié soigneusement dans le contexte des rapports entre ce bureau et le Commissariat à l'information du Canada; nous en tiendrons compte le moment venu.

Recommandation 18

Le Comité recommande qu'aucun pouvoir de rendre des ordonnances ne soit octroyé pour l'instant à la commissaire fédérale à la protection de la vie privée.

l'Alberta et la Colombie-Britannique), qui habilitent les commissaires, dans certaines circonstances, à rendre des décisions exécutoires. Ceux-ci, que l'on qualifie d'« ombudsmans munis d'un bâton », ont rarement recours à ce pouvoir; cependant, l'existence de ce pouvoir inciterait fortement à régler les questions de façon raisonnable et contribuerait à favoriser l'efficacité globale des commissaires.

Lors de sa comparution devant le Comité, David Loukidelis, commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, a exprimé l'avis suivant concernant le pouvoir de rendre des ordonnances :

> Comme vous l'avez dit, c'est également le cas en vertu du PIPA, la loi destinée au secteur privé, qui nous a donné ce pouvoir depuis 2004. Je dois cependant souligner, à titre personnel et compte tenu de l'expérience de notre Commissariat, que ce n'est pas du tout le moyen que nous privilégions. [...] Depuis la mise en vigueur du PIPA, il y a environ trois ans, je n'ai pris que sept ordonnances en vertu de cette Loi. Nous avons réglé tous les autres cas au moyen d'une approche de type médiation semblable, sous tous les aspects importants, à celles qu'ont adoptées ma collègue fédérale ici à Ottawa et les autres commissaires provinciaux. (29 novembre 2006)

La plupart des entreprises et des organisations qui ont abordé cette question disent préférer le maintien du modèle de l'ombudsman qui offre un processus de résolution des différends qui est souple, informel, accessible et économique. Il reste d'ailleurs possible de s'adresser aux tribunaux pour obtenir un examen officiel et exécutoire. Autrement dit, le modèle actuel maintient l'équilibre entre le droit du particulier à la protection de ses renseignements personnels et le droit de l'organisation de faire une utilisation légitime de ces renseignements à des fins commerciales. Les organisations préfèrent travailler en collaboration avec le Commissariat à la protection de la vie privée pour mieux comprendre ce qui est nécessaire et ce qui ne l'est pas afin d'assurer une protection raisonnable et appropriée des renseignements personnels. Ce modèle, axé sur la collaboration avec les parties afin de résoudre les questions, semble plus productif qu'une approche axée sur les plaintes de nature accusatoire et l'instruction d'accusations de violation de la Loi.

John Gustavson, de l'Association canadienne du marketing, voit plusieurs avantages au modèle de l'ombudsman :

> Les résultats des dernières années démontrent amplement que le modèle de médiateur est très bien parvenu à promouvoir et protéger les droits à la vie privée des Canadiens. Les organisations ayant fait l'objet de plaintes se sont invariablement montrées prêtes à suivre les instructions du Commissariat à la protection de la vie privée. Nous pensons également que le rôle de défenseur du Commissariat suppose intrinsèquement une certaine partialité qui le rend plus compatible avec celui d'un médiateur. Mais la réalité — et c'est l'aspect primordial — est que l'influence du Commissariat est très bien étayée par son pouvoir discrétionnaire de publier les empiétements sur la vie privée et la possibilité qu'il a de demander des ordonnances contraignantes à la Cour fédérale. (4 décembre 2006)

POUVOIRS DE LA COMMISSAIRE FÉDÉRALE À LA PROTECTION DE LA VIE PRIVÉE

1. Pouvoir de rendre des ordonnances

Comme nous l'avons signalé au début du rapport[26], la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)* est fondée sur le modèle de l'ombudsman puisque la fonction première de la commissaire à la protection de la vie privée est de faire enquête sur les plaintes d'allégation d'atteinte à la vie privée en vertu des droits que confère la Loi, et de formuler des recommandations. La Cour suprême du Canada, dans l'affaire *Lavigne c. Canada (Commissariat aux langues officielles*[27], décrit le rôle de l'ombudsman comme suit :

> L'ombudsman n'est pas l'avocat du plaignant. Il a le devoir d'examiner les deux côtés du litige, apprécier les torts et recommander les moyens d'y remédier. Il privilégie la discussion et l'entente à l'amiable.

Ainsi, la commissaire à la protection de la vie privée est habilitée à enquêter, à déposer des plaintes, à mener une vérification et à rendre publique de l'information sur les pratiques de gestion des renseignements personnels d'une organisation, mais la Loi ne lui confère pas le pouvoir de rendre des ordonnances.

Des témoins ont réclamé la modification de la LPRPDE afin de conférer à la commissaire le pouvoir de rendre des ordonnances. Ils ont fait valoir que ce pouvoir faciliterait le respect de la LPRPDE, réduirait le coût du processus actuel et les retards, et établirait une solide jurisprudence qui permettrait tant aux particuliers qu'aux organismes de mieux comprendre leurs droits et leurs responsabilités. M. Colin Bennett, professeur à l'Université de Victoria, dit craindre que le modèle de l'ombudsman ne soit pas le meilleur pour une loi qui s'applique au secteur privé :

> La leçon que je tire de mon expérience est que le modèle de l'ombudsman, qui est très utile pour la médiation et la résolution de différends entre des particuliers et des organismes, ne convient peut-être pas dans un cas comme celui-ci, quand il s'agit simplement de sensibiliser un organisme au fait qu'il doit respecter la loi ou la réglementation. En conséquence, je crois qu'il y a un décalage entre certains des buts de la loi et le modèle de l'ombudsman utilisé pour la faire appliquer. (22 novembre 2006)

Les partisans de l'octroi de ce pouvoir à la commissaire à la protection de la vie privée ont aussi fait valoir que trois provinces sont dotées de lois essentiellement similaires à la loi fédérale concernant la protection de la vie privée dans le secteur privé (le Québec,

---

26 Aperçu de la Loi.

27 *Lavigne c. Canada (Commissariat aux langues officielles),* [2002] 2 R.C.S. 733, au paragraphe 39.

ensemble de lignes directrices appelées outils de sensibilisation à la LPRPDE (OSAL). M. Wayne Halstrom, de l'Association dentaire canadienne (ADC), a formulé les commentaires suivants au sujet de l'initiative des OSAL :

> L'ADC a apprécié que le gouvernement fédéral conçoive une initiative fournissant à nos membres l'information nécessaire pour comprendre leurs obligations découlant de la LPRPDE au lieu de simplement donner un avis juridique sur la façon dont la LPRPDE s'appliquerait aux dentistes. L'ADC a fait partie du groupe de travail qui s'est réuni régulièrement avec les représentants du Commissariat à la protection de la vie privée et des ministères de la Justice, de la Santé et de l'Industrie pour créer des outils de sensibilisation à la LPRPDE pour le secteur de la santé ou, comme on l'a déjà mentionné, l'initiative des OSAL. Ce processus a produit le contenu final qui sert de base à l'interprétation de la LPRPDE par le gouvernement fédéral, c'est-à-dire une série de questions et de réponses simples qui clarifient, entre autres, les exigences relatives au consentement, à la communication des renseignements personnels sur la santé aux compagnies d'assurances privées, à la sauvegarde des données dans les bureaux, et aux demandes de modification des renseignements figurant sur les fiches dentaires. (13 décembre 2006)

L'ADC, l'Association médicale canadienne et l'Association des pharmaciens du Canada se sont toutes exprimées en faveur de l'initiative des OSAL, mais elles ont aussi recommandé de donner un caractère juridique au document des OSAL ou de l'intégrer d'une façon ou d'une autre à la LPRPDE. Dans son mémoire au Comité, Inforoute Santé du Canada inc. a aussi souligné que l'examen actuel fournit l'occasion de clarifier l'application de la LPRPDE dans le secteur des soins de santé[25].

Le Comité est sensible à la volonté de donner plus de clarté et de cohérence à l'application de la LPRPDE aux renseignements personnels sur la santé; cependant, nous ne sommes pas convaincus de l'intérêt d'ajouter encore une autre annexe à la Loi, surtout que le document des OSAL est essentiellement un feuillet de questions et de réponses destiné à aider à comprendre la LPRPDE et non à servir de conseils juridiques. Le Comité recommande par conséquent que le gouvernement consulte encore les parties prenantes du secteur de la santé ainsi que le Commissariat à la protection de la vie privée afin de déterminer quels éléments des OSAL, s'il en est (par exemple ce qui concerne le consentement implicite), peuvent être inscrits dans le cadre législatif de la LPRPDE.

Recommandation 17

Le Comité recommande que le gouvernement consulte les membres du secteur des soins de santé et le Commissariat à la protection de la vie privée du Canada afin de déterminer quels éléments du document sur les outils de sensibilisation à la LPRPDE pourraient être énoncés sous forme législative.

---

[25] Février 2007.

coopération et de développement économiques (OCDE) sur la sécurité de l'information et de la vie privée, dont le but est de relever les défis transfrontaliers que pose l'application effective des lois sur la protection de la vie privée.

Le Comité convient avec la commissaire à la protection de la vie privée qu'il n'est pas nécessaire de modifier la LPRPDE en ce qui concerne la circulation transfrontalière de renseignements personnels. À notre avis, la Loi renferme déjà des exigences suffisantes en matière de responsabilité et offre la souplesse voulue aux entreprises pour que les renseignements personnels soient dûment protégés lorsqu'ils franchissent nos frontières. Nous encourageons toutefois la commissaire à poursuivre son travail auprès de différents organismes et au sein du gouvernement fédéral, afin que cette question reçoive toute l'attention qu'elle mérite.

Recommandation 16

Le Comité recommande qu'aucune modification ne soit apportée à la LPRPDE en ce qui concerne la circulation transfrontalière de renseignements personnels.

RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ

Même si la LPRPDE est entrée en vigueur le 1er janvier 2001, elle n'est applicable aux renseignements personnels sur la santé que depuis le 1er janvier 2002, en raison des amendements qui y avaient été apportés à l'état du projet de loi (C-6). Dans son rapport de décembre 1999, le Comité sénatorial permanent des affaires sociales, des sciences et de la technologie a constaté l'incertitude entourant l'application aux renseignements personnels sur la santé des dispositions du projet de loi C-6 visant à protéger la vie privée.

Le Comité sénatorial estimait nécessaire, afin de dissiper l'incertitude, d'apporter des précisions et d'ajouter des mesures législatives. Il jugeait important en particulier d'adopter des dispositions plus précises concernant, par exemple, le consentement éclairé et l'utilisation à une fin secondaire des renseignements personnels sur la santé. Le Comité sénatorial avait recommandé par conséquent que le projet de loi soit amendé pour y inclure une définition des « renseignements personnels sur la santé » et que l'application de la Loi à ce type de renseignement soit suspendue pour une période d'un an après l'entrée en vigueur du projet de loi. Le Comité sénatorial espérait que cette suspension temporaire de la partie I du projet de loi inciterait les intervenants et les gouvernements à trouver une solution appropriée pour la protection des renseignements personnels sur la santé.

D'après les témoignages recueillis par le Comité actuel lors de son examen de la LPRPDE, ce sursis dans l'application de la LPRPDE aux renseignements personnels sur la santé a permis au gouvernement fédéral de travailler en collaboration avec le milieu de la santé, ainsi que le Commissariat à la protection de la vie privée, à l'élaboration d'un

La B.C. Freedom of Information and Privacy Association et la B.C. Civil Liberties Association nous ont aussi rappelé les questions suscitées en Colombie-Britannique par le transfert aux États-Unis du traitement de dossiers médicaux et par les inquiétudes exprimées au sujet de la portée du *U.S. Patriot Act*. Adoptée dans la foulée des événements du 11 septembre 2001, cette mesure législative a pour but d'accroître la capacité du gouvernement américain de mener des fouilles et de saisir des documents, ou d'en exiger la communication. Le gouvernement de la Colombie-Britannique a finalement modifié sa Loi sur la protection des renseignements personnels dans le secteur public pour donner suite aux préoccupations exprimées concernant la possibilité que des renseignements personnels soient divulgués sans autorisation à des autorités américaines. Au moment de sa comparution devant le Comité, le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, David Loukidelis, a parlé du problème de l'impartition en Colombie-Britannique et a expliqué la distinction qu'il convient de faire, à son avis, entre le secteur public et le secteur privé en ce qui concerne la protection des renseignements qui sont transférés outre-frontière :

> Trois semaines avant le dépôt de notre rapport qui avait abouti à cette conclusion, l'Assemblée législative provinciale a décidé de modifier la Loi sur l'accès à l'information et la protection des renseignements personnels de la Colombie-Britannique pour établir d'une façon encore plus claire que les ordonnances de tribunaux étrangers n'avaient pas d'effet extraterritorial au Canada et pour imposer aux organismes publics de la Colombie-Britannique quelques autres exigences liées à la protection des renseignements personnels.
>
> Aucune modification de ce genre n'a été apportée au PIPA, c'est-à-dire à la loi sur la protection des renseignements personnels dans le secteur privé. Dès le départ, j'avais établi une nette distinction entre le secteur public — à l'égard duquel les citoyens n'ont pas le pouvoir de consentir ou non à la décision prise par le gouvernement de donner à contrat la prestation de service public touchant leurs renseignements médicaux personnels — et le secteur privé où, en principe et en pratique aussi, à mon avis, les gens ont leur mot à dire. S'ils ne sont pas satisfaits des pratiques de l'entreprise en matière de renseignements personnels, ils peuvent toujours s'adresser ailleurs pour obtenir les biens et les services dont ils ont besoin. Je crois que cette distinction est bien réelle et qu'elle justifie un traitement différent, selon qu'il s'agit du secteur public ou du secteur privé. (29 novembre 2006)

La commissaire fédérale à la protection de la vie privée ne voit pas non plus la nécessité de modifier la loi fédérale sur la protection des renseignements personnels dans le secteur privé pour statuer sur l'impartition de données. À son avis, la meilleure façon de résoudre cette question consiste à se reporter au principe de responsabilité de la LPRPDE ainsi qu'aux lignes directrices actuelles du Conseil du Trésor concernant l'impartition[24]. La commissaire a souligné qu'elle participe aussi aux pourparlers sur cette question à l'échelle internationale. Par exemple, elle préside un Groupe de travail de l'Organisation de

---

[24] « Protéger les renseignements personnels — Un impératif : La stratégie fédérale visant à répondre aux préoccupations suscitées par la USA Patriot Act et le flux de données transfrontière », Secrétariat du Conseil du Trésor, http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/pm-prp/pm-prp_f.asp.

prévoit que cette responsabilité s'applique aussi aux renseignements confiés à une tierce partie aux fins de traitement. Dans son mémoire au Comité, l'Association canadienne de la technologie de l'information (ACTI) résume le point de vue du monde des affaires :

> Le principe de responsabilité contenu dans la LPRPDE exige que les entreprises qui font des affaires au Canada fassent preuve de transparence et informent le public de leurs pratiques en matière de protection des renseignements personnels. Il exige aussi qu'elles concluent des ententes contractuelles pour assurer une protection similaire aux renseignements personnels transférés à l'étranger. À ce chapitre, la LPRPDE, de même que le droit des contrats et des mandats, tiennent compte des réalités commerciales, juridiques et technologiques d'ordre pratique[…] L'imposition de restrictions accrues à l'égard de la circulation transfrontalière de renseignements personnels en vertu de la LPRPDE pourrait nuire à la compétitivité des entreprises canadiennes sur la scène mondiale. (11 décembre 2006)

D'autres témoins par contre ont réclamé la mise en œuvre de mécanismes plus rigoureux de protection des renseignements personnels qui s'appliqueraient au partage transfrontalier de renseignements par le secteur privé. Certains ont invoqué des arguments en faveur de l'adoption de règles précises pour protéger les renseignements personnels transférés à l'extérieur du pays et cité l'exemple de la *Loi sur la protection des renseignements personnels dans le secteur privé*[23] en vigueur au Québec, qui oblige toute personne qui communique des renseignements au sujet de citoyens québécois à des personnes à l'extérieur de la province à prendre tous les moyens raisonnables pour s'assurer que les renseignements ne seront pas communiqués à des tiers sans le consentement des principaux intéressés, sauf dans les cas prévus par la loi. Dans son mémoire au Comité, Brian Bowman, de l'Association du Barreau canadien, a formulé à ce sujet un certain nombre de propositions à examiner :

> La LPRPDE devrait prévoir des exigences préventives appropriées visant à protéger les renseignements lorsqu'ils sont transférés de l'autre côté de la frontière. Nous avons considéré au préalable de nombreuses solutions de rechange afin de réaliser cet objectif, comme une exigence obligeant les organisations qui transfèrent des renseignements à des entités étrangères à établir des ententes écrites visant à assurer la sécurité et la protection des renseignements contre la divulgation ou l'accès non autorisé conformément aux lois canadiennes. […] Dans son mémoire précédent, la Section de l'ABC a également analysé des options en vue d'une exigence en matière d'avis ou de consentement pour les renseignements transférés de l'autre côté d'une frontière. Chacune de ces options se traduirait par la fourniture d'un type d'avis aux personnes dont les renseignements personnels seraient transférés à l'extérieur du Canada ou par l'obtention de leur consentement. La modification de la LPRPDE afin de mettre en œuvre une exigence en matière d'avis ou de consentement pour le transfert transfrontalier de renseignements doit être considérée soigneusement quant aux avantages et aux désavantages d'une telle approche. (11 décembre 2006)

---

[23] Article 17.

l'Association, il faut préciser quand les mineurs peuvent donner un tel consentement et il faudrait envisager de fixer un âge minimum, en deçà duquel le consentement ne peut être accordé sans l'approbation des parents. Elle recommande que la LPRPDE soit modifiée afin de préciser que les mineurs peuvent consentir à la collecte, à l'utilisation et à la communication de leurs renseignements personnels s'ils comprennent la nature du consentement accordé et ses conséquences et que, en deçà d'un certain âge (13 ans, par exemple), le consentement doit provenir du père, de la mère ou du tuteur légal.

Dans son document de fond intitulé Examen, prévu par la loi, de la Loi sur les renseignements personnels et les documents électroniques : aperçu de la consultation du CPVP[22], la commissaire à la protection de la vie privée mentionne qu'un groupe de défense des droits des consommateurs a abordé la question des renseignements personnels des mineurs, mais elle n'a pas pris position sur la nécessité de modifier la Loi à cet égard. Il se peut qu'elle ait évité de se prononcer parce qu'il incombe aux provinces d'établir l'âge auquel les enfants sont capables d'agir de façon indépendante. Néanmoins, le Comité estime que la question du consentement à l'égard de la collecte, de l'utilisation et de la communication des renseignements personnels de mineurs dans un contexte commercial est suffisamment importante pour mériter une étude plus approfondie, ainsi que des commentaires de la part de la commissaire à la protection de la vie privée et d'autres intervenants.

Recommandation 15

Le Comité recommande que le gouvernement examine la question du consentement des mineurs concernant la collecte, l'utilisation et la communication de leurs renseignements personnels dans un contexte commercial, en vue de modifier la LPRPDE à cet égard.

IMPARTITION DE DONNÉES (CIRCULATION TRANSFRONTALIÈRE DE RENSEIGNEMENTS PERSONNELS)

Dans l'actuel contexte de haute technologie et de mondialisation des échanges, l'impartition du traitement des données devient de plus en plus systématique. Cette pratique toujours plus répandue nous incite toutefois à nous demander si les renseignements personnels des Canadiens qui sont communiqués à des organisations non canadiennes sont aussi bien protégés à l'étranger qu'ils le sont au Canada. La plupart des entreprises estiment que la LPRPDE offre actuellement une protection suffisante à cet égard. Certains évoquent le principe de responsabilité énoncé dans la LPRPDE (principe 1, annexe 1), qui stipule que toute organisation est responsable des renseignements personnels qu'elle a en sa possession. De façon précise, le principe 4.1.3

---

22 Voir la note en bas de page 14.

renseignements personnels sur les enfants. Elle décrit des sites Web très en vogue qui offrent aux enfants la possibilité de jouer à certains jeux, à condition de remplir des sondages de marketing.

> Il s'agit d'enfants de 9 ans qui jouent. Ils ne communiquent pas de l'information à des fins commerciales. Pourtant, le genre de loi que nous avons mise en place permet aux sociétés de créer cette sorte d'environnement et d'user d'un mécanisme de consentement assez douteux pour recueillir de l'information et lui donner la forme d'un bien commercial. (29 novembre 2006)

Philippa Lawson, de la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC), a exhorté le Comité à recommander que la LPRPDE soit modifiée afin d'établir des limites spéciales concernant la « collecte d'information auprès des enfants dont la crédulité et l'ignorance peuvent facilement être exploitées par des intérêts commerciaux[20] ». La CIPPIC recommande d'inclure dans la Loi des règles spéciales limitant la collecte, l'utilisation et la communication des renseignements personnels des enfants, ainsi que des sanctions strictes en cas d'infraction. L'Association canadienne du marketing a d'ailleurs fait état à cet égard du *Code canadien de pratiques pour la protection des consommateurs dans le commerce électronique*.

En réponse à une discussion sur la collecte de renseignements personnels sur les enfants, le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, David Loukidelis, a formulé les commentaires suivants, disant que des mesures législatives ont été prises aux États-Unis, mais que la question est encore à l'étude au Canada :

> Les enquêtes auprès des enfants soulèvent clairement des questions très délicates au sujet de la capacité des jeunes de comprendre ce à quoi ils s'engagent lorsqu'ils donnent des renseignements. Ces questions ont été jugées assez délicates par le Congrès des États-Unis pour qu'il adopte en 1998 le Children's *Online Privacy Protection Act* sur la protection des renseignements personnels donnés en ligne par des enfants. Au Canada, notre expérience dans ce domaine reste assez limitée. De mon côté, j'espère qu'en Colombie-Britannique, nous pourrons, trois ans seulement après l'adoption de notre Loi, continuer à collaborer avec l'industrie pour assurer le respect des principes généraux dans le cas des enfants et, d'une façon plus générale, pour tous ces problèmes technologiques. J'espère que notre Loi donnera de bons résultats dans sa forme actuelle, sans qu'il soit nécessaire de changer radicalement notre approche à l'égard de certaines de ces technologies. (29 novembre 2006)

L'Association du Barreau canadien (ABC) présente, dans le mémoire préparé en prévision de l'examen de 2006 de la LPRPDE, un bref examen des questions touchant le consentement des mineurs[21]. L'ABC affirme que l'on ne sait pas vraiment si les mineurs peuvent consentir à des activités en ligne sans le consentement de leurs parents. Selon

---

20 6 décembre 2006.

21 Voir la note en bas de page 16, p. 43-44.

> Pour comprendre les conséquences découlant de cette modification, il convient de connaître la signification du mot « recueillir ». Alors que le mot « utilisation » est lié à l'administration et à différentes autres utilisations des renseignements personnels existants qui ont été recueillis antérieurement, le mot « recueillir » renvoie à l'acquisition de nouveaux renseignements qui n'existaient pas antérieurement au sein de l'organisation.
>
> Aux termes de la modification apportée par la *Loi sur la sécurité publique*, les organisations peuvent désormais recueillir de nouveaux renseignements sur leurs clients et leurs employés ou sur toute autre partie lorsqu'elles jugent que l'intérêt national est en jeu et aux fins de les divulguer ultérieurement à une agence de sécurité.
>
> Cela peut engendrer de nombreux abus des droits individuels à la protection de la vie privée. (6 février 2007, mémoire, p. 8)

La commissaire à la protection de la vie privée, dans son mémoire au Comité, s'est dite très préoccupée par le libellé général de l'alinéa 7(1)*e*). Selon elle, cette disposition, puisqu'elle s'applique à toute organisation assujettie à la LPRPDE, a malheureusement pour effet de déléguer au secteur privé des activités d'application de la loi, sans l'obligation correspondante de rendre compte publiquement[19]. La commissaire réclame, comme elle l'a fait au moment de l'adoption de la *Loi sur la sécurité publique* de 2002, que l'alinéa 7(1)*e*) de la LPRPDE soit abrogé, ou à tout le moins que sa portée soit plus restreinte.

Dans une lettre datée du 20 mars 2007, que le président a livré personnellement le même jour, le Comité a demandé son aide au ministre de la Sécurité publique afin de régler les questions soulevées par les témoins dans ce domaine. Plus précisément, le ministre a été prié de comparaître ou de présenter ses commentaires par écrit dans un délai d'environ une semaine, afin que le Comité puisse remettre son rapport à temps à la Chambre des communes. Comme le ministre n'a pas répondu, le Comité, compte tenu des témoignages recueillis et après un débat réfléchi, formule la recommandation qui suit :

Recommandation 14

Le Comité recommande que l'alinéa 7(1)*e*) soit retiré de la LPRPDE.

RENSEIGNEMENTS PERSONNELS SUR DES MINEURS

Certains témoins voudraient inclure dans la LPRPDE des règles spéciales conçues pour protéger les enfants contre la collecte, l'utilisation ou la communication abusive de leurs renseignements personnels. Valerie Steeves, professeure à l'Université d'Ottawa, a expliqué au Comité les moyens subtils utilisés sur Internet pour recueillir des

---

[19] Note de bas de page 14.

Recommandation 12

Le Comité recommande que l'on envisage de préciser ce que l'on entend par « autorité légitime » à l'alinéa 7(3)*c*.1) de la LPRPDE et que la formule introductive du paragraphe 7(3) soit modifiée pour se lire comme suit : « Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation doit communiquer des renseignements personnels à l'insu de l'intéressé et sans son consentement dans les cas suivants :[…]».

Recommandation 13

Le Comité recommande que l'expression « institution gouvernementale » aux alinéas 7(3)*c*.1) et *d*) de la LPRPDE soit éclaircie afin de préciser si elle comprend les entités municipales, provinciales, territoriales, fédérales et non canadiennes.

ii. Alinéa 7(1)*e*)

L'alinéa 7(1)*e*) a été ajouté à la LPRPDE en vertu de la *Loi sur la sécurité publique* de 2002 qui a modifié un certain nombre de lois fédérales en 2004, dans la foulée des événements du 11 septembre 2001 aux États-Unis. Avant 2004, les organisations assujetties à la LPRPDE étaient habilitées à *communiquer* des renseignements personnels à l'insu de l'intéressé et sans son consentement pour des motifs liés à la sécurité nationale, à la défense du Canada et à la conduite des affaires internationales ou quand la Loi l'exigeait (alinéa 7(3)*c*.1) et sous-alinéas 7(3)*d*)(ii) et 7(3)(i)). En vertu des modifications imposées par la *Loi sur la sécurité publique*, les organisations peuvent maintenant aussi *recueillir* et *utiliser* les renseignements personnels à l'insu de l'intéressé et sans son consentement, en vue de les communiquer aux fins précitées. Or, c'est ce nouveau pouvoir de collecte qui inquiète particulièrement les défenseurs de la vie privée.

Le Comité a entendu des particuliers ainsi que des organisations de protection de la vie privée déclarer que l'alinéa 7(1)*e*) de la LPRPDE a le défaut non seulement de contourner le régime du consentement soigneusement construit par la Loi, mais aussi d'effacer la séparation entre le secteur privé et l'application de la loi[18]. Murray Long, consultant en matière de protection de la vie privée, a formulé les commentaires suivants au sujet de la disposition :

---

[18] Colin Bennett, Présentation à un Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 22 novembre 2006, p. 13.

des dispositions de la LPRPDE concernant la communication volontaire par des entreprises de renseignements personnels non sensibles, nuit à l'application de la Loi. M. Clayton Pecknold, de l'Association canadienne des chefs de police, a expliqué le problème au Comité de la manière suivante :

> Pour prendre un autre exemple, un policier peut débuter une enquête sur une disparition et chercher à établir s'il y a eu crime. Il devra peut-être demander l'aide d'une institution financière pour savoir si la personne disparue a acheté de l'essence dans une station-service ou si elle a utilisé une carte de crédit, ou encore il devra établir si elle possède un téléphone cellulaire d'une compagnie donnée. Pour obtenir ces renseignements, nous invoquons l'alinéa 7(3)*c*.1) qui permet d'obtenir le renseignement en mentionnant la source de l'autorité légitime, comme on vous l'a dit tout à l'heure. Néanmoins, nous constatons de plus en plus que certaines entreprises considèrent que l'autorité légitime doit prendre la forme d'un mandat ou d'une ordonnance du tribunal. Nous vous faisons respectueusement remarquer que cette interprétation n'est pas, selon nous, conforme aux intentions du législateur. Cette interprétation qui témoigne certainement d'un désir légitime de protéger la vie privée des clients de l'entreprise est beaucoup trop limitative et va à l'encontre de l'intention de l'alinéa 7(3)*c*.1). (13 février 2007)

L'ACCP, le Centre canadien de ressources pour les victimes de crimes et la GRC ont tous recommandé que l'alinéa 7(3)*c*.1) soit modifié afin de préciser que le principe d'autorité légitime n'oblige pas à produire une ordonnance judiciaire afin d'obtenir la communication de renseignements.

Le Comité convient que la notion d'autorité légitime, aux fins de la communication en vertu de l'alinéa 7(3)*c*.1), suscite des préoccupations valables. Manifestement, il faut prévoir autre chose qu'une autorisation judiciaire en vertu de cette disposition, étant donné que l'alinéa 7(3)*c*) prévoit déjà la communication de renseignements à l'insu et sans le consentement de l'intéressé, sur production d'une assignation ou d'un mandat. Nous estimons donc important de préciser ce que l'on entend par « autorité légitime » aux fins de l'alinéa 7(3)*c*.1), à l'intention tant des organisations que des organismes d'application de la loi. De plus, le Comité estime qu'il faut envisager de remplacer le mot « peut » dans la formule introductive du paragraphe 7(3) afin que la disposition soit de nature obligatoire plutôt que facultative. Nous comprenons, étant donné la nature facultative du paragraphe 7(3) et la façon dont ce dernier s'insère dans le cadre de la Loi, qu'il faudra peut-être limiter l'application obligatoire aux dispositions de communication qui visent des questions d'application de la loi et de sécurité nationale.

Le Comité convient aussi qu'il faut préciser ce que désigne l'expression « institution gouvernementale » aux alinéas 7(3)*c*.1) et *d*) de la LPRPDE. Les organisations devraient plus particulièrement savoir si le terme comprend les entités municipales, provinciales, territoriales et fédérales ainsi que les entités non canadiennes.

Recommandation 11

Le Comité recommande que la LPRPDE soit modifiée par l'ajout de nouvelles exceptions aux exigences en matière de consentement pour permettre la collecte de renseignements à des fins personnelles, familiales et d'intérêt public, de façon à harmoniser l'approche fédérale avec celles adoptées par le Québec, l'Alberta et la Colombie-Britannique dans leurs lois respectives sur la protection des renseignements personnels dans le secteur privé.

G. Application de la loi et sécurité nationale

i. Alinéa 7(3)*c.*1)

L'alinéa 7(3)*c.*1) de la LPRPDE habilite les organisations à communiquer des renseignements personnels aux institutions gouvernementales, à l'insu et sans le consentement du principal intéressé et sans autorisation judiciaire, dans des situations précises, aux fins de l'application de la loi et de la sécurité nationale. Des témoins s'inquiètent de ce que désigne « institution gouvernementale » dans cette disposition et proposent que des précisions soient apportées, car les renseignements sont communiqués à ce type d'entité sans que la personne concernée le sache ou y consente.

L'Association du Barreau canadien, par exemple, a recommandé d'ajouter à la LPRPDE une définition d'« institution gouvernementale » afin de préciser si, aux fins de la communication, le terme comprend ou non les entités municipales, provinciales, territoriales, fédérales et non canadiennes. La Clinique d'intérêt public et de politique d'Internet du Canada (CPPIC) insiste pour que l'expression « institution gouvernementale » figurant aux alinéas 7(3)*c.*1) et *d*) s'applique uniquement aux institutions gouvernementales canadiennes, étant donné les inquiétudes que suscitent chez la population canadienne le niveau d'impartition à l'étranger du traitement des renseignements, et les pouvoirs qu'ont les agences étrangères d'obtenir ces données sur demande auprès d'entreprises privées. Ainsi, les gouvernements étrangers qui souhaitent obtenir des renseignements sur des Canadiens devront passer par les entités gouvernementales canadiennes.

Une autre question soulevée relativement à l'alinéa 7(3)*c.*1) portait sur le sens « d'autorité légitime ». Certains témoins, comme les représentants de la BC Freedom of Information and Privacy Association et de la BC Civil Liberties Association, sont d'avis que les entreprises privées devraient exiger que la police ou l'organisme d'enquête concerné produise une ordonnance judiciaire (sauf dans des cas exceptionnels ou urgents) avant de divulguer un renseignement personnel en vertu de cette disposition. Par contre, selon les représentants de l'Association canadienne des chefs de police (ACCP), du Centre canadien de ressources pour les victimes de crimes et de la GRC, l'interprétation stricte

de ces clients s'attendent à ce que les banquiers aident à les prévenir. Cependant, en vertu de la législation actuelle, même si les employés des succursales bancaires veulent apporter leur aide, ils ne sont pas autorisés à le faire, car aucune exception ne s'applique à ces situations. Nous recommandons une exemption supplémentaire en ce qui a trait à la communication sans consentement lorsque c'est dans l'intérêt public. (30 janvier 2007)

L'ABC recommande que le paragraphe 7(3) de la LPRPDE soit modifié de façon à permettre la communication de renseignements personnels aux autorités compétentes, aux proches ou à une personne désignée par le principal intéressé lorsque la divulgation de cette information est dans l'intérêt du principal intéressé ou dans l'intérêt public.

Dans son mémoire à Industrie Canada en prévision du présent examen de la Loi par le Comité[17], l'Association du Barreau canadien recommande de prendre certains facteurs en considération au moment d'évaluer la pertinence de s'appuyer sur un consentement obtenu indirectement par l'intermédiaire d'une autre personne. Par exemple, la nature de la transaction, la sensibilité des renseignements personnels, la nature du lien qui unit la personne à celle qui confirme son consentement et la mesure à laquelle la collecte, l'utilisation ou la communication profite à l'intéressé sont tous des facteurs qui devraient figurer dans la Loi au nombre des critères d'évaluation.

La commissaire à la protection de la vie privée est d'avis que certaines exceptions très précises devraient être envisagées à cet égard en ce qui concerne les exigences en matière de consentement. Elle a mentionné, à ce sujet, les exemples suivants : communication de renseignements à la famille d'une personne blessée, malade ou décédée, ou encore nécessité d'aviser dans des situations d'urgence en milieu communautaire.

Comme il est mentionné au début du présent rapport, le Comité est conscient de la nécessité d'harmoniser la LPRPDE aux lois provinciales en matière de protection des renseignements personnels dans le secteur privé. C'est là un cas où il faudrait prendre en considération les dispositions pertinentes des lois du Québec, de l'Alberta et de la Colombie-Britannique. Le Comité hésite toutefois à recommander l'utilisation de l'expression « intérêt public » dans ce contexte, étant donné son ambiguïté possible et le fait que nous avons entendu beaucoup de témoignages au sujet de l'imprécision des termes ou du manque de clarté des dispositions actuelles de la LPRPDE. Cela dit, nous sommes conscients que le recours à une expression générale comme « intérêt public » peut être nécessaire pour offrir la souplesse voulue à l'application d'une telle exemption.

---

[17] Ibid., p. 42-43.

disposition de la LPRPDE stipule qu'une personne puisse donner son consentement au nom d'une autre, si cette autre personne peut se prévaloir d'un produit ou d'un service dans le cadre duquel ses renseignements personnels ont été fournis. À cet égard, certains ont évoqué le paragraphe 8(2) du *Personal Information Protection Act* de la Colombie-Britannique, qui est libellé comme suit :

> Le particulier est réputé consentir à la collecte, à l'utilisation ou à la communication de renseignements personnels pour obtenir les avantages ou la protection découlant d'une assurance, d'une pension ou d'un régime, contrat ou police semblable lorsque les conditions suivantes sont remplies :
>
> a) il est bénéficiaire ou a un intérêt comme assuré au titre du régime, de la police ou du contrat;
>
> b) il n'est pas le requérant ou le proposant aux fins du régime, de la police ou du contrat.

Advocis recommande d'envisager la possibilité de s'inspirer du libellé de l'alinéa 14*a*) du *Personal Information Protection Act* de l'Alberta pour permettre aux conseillers financiers de recueillir de l'information au sujet de tierces parties au moment d'élaborer un plan financier pour leurs clients. Le paragraphe 14*a*) autorise une organisation à recueillir des renseignements personnels sans le consentement de l'intéressé lorsqu'« une personne raisonnable estimerait que la collecte des renseignements est manifestement dans l'intérêt du particulier et [qu']il est impossible d'obtenir le consentement de celui-ci en temps opportun ou [qu']il est raisonnable de s'attendre à ce que le particulier en question donne son consentement ».

L'Association des banquiers canadiens (ABC) a évoqué des situations comme les catastrophes naturelles, lorsque les membres d'une famille veulent savoir si un proche a survécu ou veulent obtenir de l'information à son sujet, et d'autres, dans le contexte du travail, où un employeur a des renseignements importants à transmettre à un employé, mais est incapable de le joindre et doit communiquer avec le plus proche parent ou la personne-ressource désignée. Les banquiers s'inquiètent également de l'incidence des abus financiers dont sont victimes les aînés et de l'incapacité de la LPRPDE de remédier à ce problème. Voici comment M. Warren Law de l'ABC a exprimé les préoccupations des banquiers à cet égard :

> Dans le contexte bancaire, une telle situation survient, par exemple, lorsqu'un banquier soupçonne un abus financier — surtout dans le cas des aînés — au moment où un client retire de l'argent de son compte. Ce client semble subir la pression de la personne qui l'accompagne où le retrait ne reflète pas ses habitudes.
>
> Avant l'entrée en vigueur de la *Loi sur la protection des renseignements personnels et les documents électroniques*, les banques pouvaient, en vertu de la common law, faire part de leurs soupçons aux autorités compétentes, à la famille du client vulnérable ou à toute autre personne responsable qui aurait pu faire enquête et empêcher l'abus. Les abus financiers des aînés sont un enjeu important au Canada. Le public et les familles

Nous n'avons pas recueilli de témoignages à ce sujet de la part d'organismes de protection de la vie privée ni de la part de la commissaire fédérale, mais nous estimons néanmoins qu'il faudrait peut-être nous demander s'il n'y a pas moyen de traiter des déclarations de témoins dans la LPRPDE autrement que par l'ajout de l'exception que nous proposons aux fins d'enquêtes (Recommandation 6) et des exceptions suivantes applicables aux procédures et instances judiciaires.

Recommandation 9

Le Comité recommande que la LPRPDE soit modifiée de façon à créer une exception — essentiellement comme celle que prévoient les Lois sur la protection des renseignements de l'Alberta et de la Colombie-Britannique — pour soustraire à l'obligation d'obtenir un consentement les renseignements auxquels une partie à une instance a légitimement accès.

Recommandation 10

Le Comité recommande que le gouvernement consulte la commissaire à la protection de la vie privée afin de déterminer s'il faut apporter d'autres modifications à la LPRPDE pour régler la question des déclarations de témoins et des droits des personnes dont les renseignements personnes sont contenues dans ces déclarations.

F. Exceptions aux exigences en matière de consentement pour la collecte de renseignements à des fins personnelles, familiales et d'intérêt public

L'alinéa 7(3)*e*) de la LPRPDE autorise la communication de renseignements personnels sans le consentement des intéressés « à toute personne qui a besoin du renseignement en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de toute personne et, dans le cas où la personne visée par le renseignement est vivante, l'organisation en informe par écrit et sans délai cette dernière ». Certains témoins estiment toutefois que la portée de cette disposition n'est pas assez large pour s'appliquer à d'autres situations qui justifieraient elles aussi l'invocation d'une exception semblable.

Le Comité a entendu le Bureau d'assurance du Canada (BAC) et la Financial Advisors Association of Canada (Advocis) affirmer qu'il serait utile de prévoir une exemption à l'obligation d'obtenir un consentement en vertu de la LPRPDE dans le cas des bénéficiaires (désignés, par exemple, par testament ou dans une police d'assurance). Le BAC a fait valoir, par exemple, qu'il arrive souvent, dans le domaine de l'assurance, qu'une personne demande une assurance et que la police d'assurance soit souscrite à son nom, mais que d'autres personnes soient nommées dans la police ou y figurent à titre d'assurés supplémentaires ou de bénéficiaires. Le BAC demande donc à ce qu'une

administratives engagées à la suite d'une violation d'entente, d'une dérogation à une loi fédérale ou provinciale ou d'un recours judiciaire ou une voie de droit en common law ou en equity.

Suivant une argumentation assez semblable, le Bureau d'assurance du Canada (BAC) demande qu'une exemption soit prévue pour soustraire les déclarations de témoins à l'obligation d'obtenir un consentement en vertu de la LPRPDE. Le BAC recommande que la définition de « renseignement personnel » soit révisée de manière à préciser que les renseignements personnels communiqués par une personne (« le témoin ») au sujet d'une autre (« le sujet ») soient les renseignements personnels du témoin. Il estime aussi que l'article 7 de la LPRPDE devrait être modifié de manière à permettre à une organisation, dans le cadre d'une enquête et du règlement de différends contractuels ou de réclamations pour pertes ou dommages, de recueillir, d'utiliser et de communiquer la déclaration d'un témoin à l'insu du sujet ou sans le consentement de ce dernier. Voici la justification donnée par le BAC à l'appui de ses propositions :

> À notre avis, il serait déraisonnable d'empêcher l'assureur - ainsi que le tribunal et le juré si une poursuite est entamée et l'affaire instruite - de recueillir tous les faits pertinents reliés à l'incident. Nous sommes opposés au principe selon lequel un assureur doit obtenir au préalable le consentement du réclamant ou d'un éventuel réclamant pour obtenir les déclarations des témoins. Cette position peut avoir de graves conséquences car, dans les faits, elle pourrait permettre à une personne d'empêcher une autre (le témoin) de déclarer ce qu'elle a vu ou entendu et empêcherait l'assureur, et le tribunal par ricochet, de recueillir tous les faits pertinents se rapportant à l'incident. (24 novembre 2006, mémoire, p. 4).

Le Comité convient qu'il semble y avoir certaines incohérences dans les exceptions actuellement prévues relativement à l'application des dispositions de la LPRPDE exigeant l'obtention d'un consentement, et qu'il serait préférable d'assouplir l'approche adoptée à cet égard. Nous avons entendu divers témoignages à ce sujet. De façon précise, en ce qui concerne les procédures ou instances judiciaires, le Comité croit que les dispositions de la LPRPDE sur la protection des renseignements personnels ne devraient pas nuire au bon déroulement d'une instance judiciaire et qu'il y a peut-être lieu d'apporter une modification pour soustraire à l'obligation d'obtenir un consentement les renseignements nécessaires aux fins d'une procédure judiciaire. Il faudrait, à cet égard, chercher à harmoniser la LPRPDE aux Lois de la Colombie-Britannique et de l'Alberta.

Le Comité juge préoccupants aussi les témoignages recueillis au sujet des déclarations de témoins et des renseignements personnels qu'elles contiennent. Nous savons que les compagnies d'assurance, lorsqu'elles font enquête pour régler un sinistre, sont aux prises avec la question de savoir si elles doivent obtenir le consentement du réclamant ou d'un éventuel réclamant quand des renseignements à son sujet sont contenues dans une déclaration de témoin. De plus, des assureurs nous ont signalé qu'ils hésitent à donner l'accès aux déclarations de témoins aux réclamants qui affirment avoir le droit de consulter ces documents du fait que ceux-ci constituent des renseignements personnels qui les concernent.

Recommandation 8

Le Comité recommande que l'on envisage de modifier la LPRPDE en ce qui concerne la relation entre mandants et agents. Il conviendrait de se reporter au paragraphe 12(2) de la Loi sur la protection des renseignements personnels de la Colombie-Britannique pour formuler cette modification.

E. Procédure et instance judiciaires

En ce qui concerne les préoccupations exprimées par les témoins au sujet de la façon dont la LPRPDE s'applique aux activités d'application de la loi et d'enquête (voir la rubrique Organismes d'enquête ci-dessous), le Comité a entendu des témoignages selon lesquels il faudrait faire en sorte que la LPRPDE n'ait pas d'effet sur la procédure judiciaire. Voici ce que Brian Bowman de l'Association du Barreau canadien avait à dire à ce sujet dans son mémoire au Comité :

> La LPRPDE ne devrait avoir d'incidence ni sur les litiges préexistants, ni sur les procédures de contestation judiciaire communément acceptées et qui évoluent depuis des décennies, voire des siècles. Il faut modifier nombre des exceptions à l'exigence de consentement prévue dans la LPRPDE. Les exceptions actuelles concernant les litiges sont trop limitées et elles devraient, à tout le moins, être élargies pour éviter de nuire à des procédures de contestation bien fondées. Cette étroitesse des exceptions devient évidente dans le cadre d'enquêtes, de communications à sens unique, de collecte et d'utilisation d'information sur les dettes et des restrictions de divulgation pendant un litige. En outre, elle donne lieu à un traitement inadéquat de l'ensemble des aspects du processus : plaidoyer, divulgation orale, médiation, arbitrage privé, règlements à l'amiable, communications entre avocats et autres échanges d'information non ordonnés par un tribunal. Il devrait y avoir une exclusion générale en ce qui concerne l'information qu'une partie peut obtenir en vertu de la loi, dans le cadre d'un litige, et cette exclusion devrait annuler les exceptions particulières actuellement prévues dans la LPRPDE. (11 décembre 2006)

En matière d'instance judiciaire, l'Association du Barreau canadien recommande de s'inspirer des modèles proposés dans les Lois de la Colombie-Britannique et de l'Alberta en matière de protection des renseignements personnels pour formuler les dispositions de la LPRPDE. Les articles 12, 15 et 18 de la Loi de la Colombie-Britannique autorisent la collecte, l'utilisation et la communication de renseignements personnels sans le consentement du principal intéressé, si la collecte, l'utilisation ou la communication avec son consentement risquaient de compromettre l'exactitude des renseignements personnels ou l'accès à ceux-ci et si elles sont raisonnables aux fins d'une enquête ou d'une instance. Les articles 14, 17 et 20 de la loi de l'Alberta autorisent la collecte, l'utilisation et la communication de renseignements personnels sans le consentement du principal intéressé, si la collecte, l'utilisation ou la communication sont raisonnables aux fins d'une enquête ou d'une instance. Les deux Lois définissent les termes « instance » et « instance judiciaire » comme s'appliquant aux poursuites civiles, pénales ou

Une organisation peut recueillir des renseignements personnels auprès d'une autre organisation ou en son nom sans le consentement du sujet des renseignements, si

(a) l'intéressé a déjà consenti à ce que l'autre organisation recueille les renseignements personnels, et

(b) les renseignements personnels sont communiqués ou recueillis par l'organisation uniquement :

(i) aux fins pour lesquelles les renseignements avaient été recueillis à l'origine et

(ii) pour lui permettre d'effectuer des travaux au nom de l'autre organisation. [traduction]

Dans le mémoire préparé en prévision du présent examen[16], l'Association du Barreau canadien a aussi soulevé la nécessité d'expliquer la notion d'agent contenue dans la LPRPDE. Elle signale que la règle concernant le traitement par une tierce partie qui est énoncée dans le principe 4.1.3, à l'annexe 1 de la Loi et qui prévoit que l'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie, ne précise pas explicitement si le traitement est considéré comme un transfert ou une communication, laquelle nécessiterait un consentement. De plus, l'Association estime que la Loi ne précise pas si l'exception pour les traitements est strictement limitée aux transferts de renseignements aux fins de la paye, des pensions et d'autres mesures administratives (par opposition, par exemple, au travail d'un enquêteur privé dont l'organisation a retenu les services. L'Association propose donc de modifier la LPRPDE de manière à confirmer qu'une organisation puisse recueillir, utiliser et communiquer des renseignements personnels provenant de l'organisation principale, ou en son nom, sans le consentement de l'intéressé, mais seulement si ce dernier a consenti à la collecte, à l'utilisation et à la communication des renseignements par l'organisation principale, et que les renseignements servent à exécuter des travaux au nom de cette dernière.

Le Comité pense aussi qu'il faut éliminer toute ambiguïté concernant l'existence dans la LPRPDE du lien entre mandant et agent. Étant donné que la recommandation de l'Association du Barreau canadien semble essentiellement correspondre au paragraphe 12(2) de la Loi de la Colombie-Britannique, nous recommandons que la LPRPDE soit modifiée de façon à clarifier la relation entre mandant et agent, en s'inspirant de la Loi de la Colombie-Britannique.

---

16 Association du Barreau canadien, Section nationale du droit de la vie privée et de l'accès à l'information, *Preparing for the 2006 Review of the Personal Information Protection and Electronic Documents Act*, août 2005, p. 21-24.

commissaire à la protection de la vie privée, appuient en particulier le modèle de l'Alberta; nous recommandons par conséquent l'adoption de ce modèle, assorti des améliorations proposées par la commissaire.

Recommandation 7

Le Comité recommande que la LPRPDE soit modifiée par l'ajout d'une disposition habilitant les organisations à recueillir, à utiliser et à communiquer des renseignements personnels sans consentement, aux fins de transactions commerciales. Cette modification pourra s'inspirer de la disposition contenue dans la Loi sur la protection des renseignements personnels de l'Alberta et comprendre les améliorations recommandées par la commissaire à la protection de la vie privée du Canada.

D. Relation mandant-agent

Le Bureau d'assurance du Canada (BAC) a attiré l'attention du Comité sur la question des ententes entre mandants et agents. Le BAC s'inquiète de l'absence dans la LPRPDE de dispositions donnant des précisions sur ce genre d'entente. Ainsi, dans le cadre d'une telle entente, l'agent devrait pouvoir compter sur le consentement accordé au préalable par le mandant pour exercer certaines fonctions. Dans le domaine de l'assurance, les enquêtes et les règlements d'indemnités sont parfois impartis à des bureaux d'experts en sinistres indépendants, et le BAC craint que cette impartition soit considérée comme une communication de renseignements aux fins de la Loi, de sorte qu'il faudrait un consentement distinct à l'intention de l'agent. Dans son mémoire au Comité, le BAC présente les explications suivantes :

> L'impartition de fonctions opérationnelles à des agents est un élément essentiel des pratiques commerciales de tous les secteurs des affaires. Un individu raisonnable, dont il est question à l'article 3 et au paragraphe 5(3) de la LPRPDE, s'attendrait à ce qu'un assureur, à l'instar de toute autre entreprise, impartisse certaines fonctions à des agents agissant au nom de l'assureur. Dans le cas où l'agent désirerait utiliser les renseignements personnels à ses propres fins, il lui faudrait obtenir de la part de la personne un consentement distinct pour cette utilisation distincte. (24 novembre 2006, p. 12)

Le BAC renvoie au paragraphe 12(2) du *Personal Information Protection Act* de la Colombie-Britannique comme solution possible au problème. Il propose autrement d'ajouter à la LPRPDE des définitions des termes « agent », « utilisation » et « communication ». Le libellé du paragraphe 12(2) de la Loi de la Colombie-Britannique est le suivant :

location, la fusion ou tout autre type d'acquisition ou de cession d'une organisation. Les organisations sont autorisées à communiquer des renseignements personnels, si cela est nécessaire, pour prendre une décision au sujet de la transaction et passer à l'action, mais elles sont aussi obligées de remettre ou de détruire les renseignements si la transaction n'a pas lieu.

L'article 20 du *Personal Information Protection Act* de la Colombie-Britannique prévoit essentiellement les mêmes conditions pour la communication de renseignements, mais il précise en outre que les renseignements communiqués doivent servir uniquement aux fins pour lesquelles ils ont été recueillis et que les personnes dont les renseignements personnels ont été communiqués doivent être informées de la communication et de la conclusion de la transaction commerciale.

L'Association médicale canadienne a demandé que toute nouvelle disposition concernant la vente ou le transfert d'une entreprise reconnaisse explicitement la situation particulière des renseignements des médecins et des patients, qu'elle explique ainsi :

> Les médecins s'efforcent de dispenser aux patients des soins de santé de qualité en temps opportun, tout en faisant face souvent à des exigences multiples et divergentes. Les médecins demandent donc aux législateurs de garantir que toute modification à la LPRPDÉ tiendra compte des répercussions qu'elle pourrait éventuellement avoir sur eux-mêmes ainsi que sur leurs patients. Premièrement, nous demandons l'assurance que les soins de santé soient considérés comme un domaine particulier lorsqu'il est question de la divulgation des renseignements personnels avant la cession d'une entreprise (un médecin qui cède sa pratique à un autre) parce qu'ils sont réglementés à l'échelle provinciale par l'ordre compétent. En règle générale, les médecins doivent prévenir le public du changement de propriétaire de la pratique, soit en publiant une annonce dans un journal, soit en affichant un avis dans le bureau du médecin. (13 décembre 2006)

La commissaire à la protection de la vie privée, dans son mémoire final au Comité, a préconisé la modification de la LPRPDE de façon à créer une version améliorée du modèle de l'Alberta concernant la fusion ou la vente d'entreprises. Sur le plan des améliorations, elle recommande une exigence de diligence raisonnable qui limitera au strict minimum la communication de données identifiables. De plus, après un transfert de propriété, toute personne dont les renseignements ont été transférés sans son consentement doit en être informée le plus tôt possible. Finalement, le nouveau propriétaire devrait être tenu de respecter les politiques de l'ancienne organisation concernant la protection de la vie privée jusqu'à ce que tous les intéressés aient eu la possibilité de décider s'ils veulent être en rapport avec le nouveau propriétaire.

Le Comité convient que la LPRPDE doit être modifiée afin de créer une exception aux exigences de consentement dans le cas de transactions commerciales ou de restructuration d'entreprises. En fait, nous avons pu constater qu'aucun témoin ne s'est opposé à une telle modification. Il reste toutefois à déterminer la meilleure façon de faciliter ces transactions tout en protégeant, le plus possible, la nature privée des renseignements personnels communiqués. Nous remarquons que de nombreux témoins, dont la

intéressé aux fins d'enquête, définie comme étant une enquête sur la violation d'une entente, la dérogation à une fédérale ou provinciale, ou des circonstances ou une conduite pouvant donner lieu à un recours judiciaire.

Recommandation 6

Le Comité recommande de modifier la LPRPDE pour remplacer le processus de désignation des « organismes d'enquête » par une définition du terme « enquête », semblable à celle énoncée dans les Lois de l'Alberta et de la Colombie-Britannique en matière de protection des renseignements personnels, qui prévoit la collecte, l'utilisation et la communication de renseignements personnels sans le consentement du principal intéressé, aux fins d'enquête.

C. Transactions commerciales

De nombreux représentants d'entreprises ont parlé au Comité de l'absence de dispositions dans la LPRPDE, permettant à une organisation de communiquer des renseignements personnels à des acquéreurs éventuels ou à des partenaires commerciaux, sans avoir obtenu au préalable le consentement des intéressés. Pourtant, les entreprises ont souvent besoin de prendre connaissance de ces renseignements (par exemple des listes de clients) pour évaluer si elles doivent procéder à la transaction — que ce soit une fusion, une acquisition ou la vente d'une entreprise —, et obtenir le consentement de tous les clients est un lourd processus.

Selon le Document de discussion sur l'examen de la LPRPDE de la commissaire à la protection de la vie privée[15], plusieurs provinces sont dotées de lois de protection des données, comme la *Loi sur la protection des renseignements personnels sur la santé* (LPRPS) de l'Ontario et les *Personal Information Protection Acts* (PIPA) de l'Alberta et de la Colombie-Britannique qui permettent la communication de renseignements personnels, sans avoir obtenu le consentement de l'intéressé, à des fins de transactions commerciales, sous réserve d'un rigoureux accord de confidentialité. Plusieurs témoins ont préconisé l'ajout d'une disposition semblable dans la LPRPDE, sur le modèle de celles contenues dans les Lois de l'Alberta ou de la Colombie-Britannique, afin de faciliter les transactions commerciales et de protéger le secret commercial dans un contexte de concurrence.

L'article 22 du *Personal Information Protection Act* de l'Alberta prévoit un régime de communication des renseignements personnels sans consentement lors d'une transaction commerciale, laquelle est définie de façon assez générale comme étant l'achat, la vente, la

---

15 Commissariat à la protection de la vie privée, *Document de discussion sur l'examen de la LPRPDE*, juillet 2006, Ibid.

> La Loi comporte des incohérences entre les exemptions relatives à la collecte, à l'utilisation et à la communication de renseignements personnels, qui peuvent nuire aux efforts des banques pour prévenir la fraude contre leurs clients, d'autres clients et la banque. Dans leurs efforts pour prévenir la fraude et enquêter à cet égard, les banques font face à des situations où elles ont besoin de pouvoir recueillir, utiliser et communiquer des renseignements personnels sans le consentement de l'intéressé, mais elles sont incapables de le faire en raison des incohérences de la Loi, entre les paragraphes 7(1), 7(2) et 7(3). Par exemple, bien que la Loi permette à une organisation de recueillir et de communiquer des renseignements sur la violation d'un accord, elle n'autorise pas leur usage interne dans le cours de l'enquête visant, à prévenir d'autres fraudes contre ce client, d'autres clients ou la banque. (janvier 2007, p. 4)

Pour remédier à ces préoccupations, certains témoins ont proposé que, plutôt que de désigner les organismes d'enquête par réglementation, le gouvernement pourrait ajouter à la Loi une définition d'«organisme d'enquête » afin que les organismes puissent se désigner eux-mêmes à partir d'une liste de critères. Par ailleurs, bon nombre d'organisations ont plaidé en faveur de l'élimination complète de la notion d'« organisme d'enquête » dans la LPRPDE. Elles recommandent que le Comité modifie la LPRPDE en s'inspirant des solutions adoptées par l'Alberta et la Colombie-Britannique, qui définissent le terme « enquête » dans leurs lois respectives et autorisent à cette fin la collecte, l'utilisation et la communication sans le consentement de l'intéressé. La Loi de la Colombie-Britannique fait expressément mention de la prévention de la fraude dans sa définition.

La commissaire à la protection de la vie privée croit que, malgré sa lourdeur, l'actuel mode de désignation des organismes d'enquête fonctionne bien et n'a pas besoin d'être modifié pour l'instant. Dans le document de discussion qu'elle a remis au Comité, la commissaire souligne qu'elle souscrit à l'actuel processus de désignation parce qu'il est transparent et permet d'exercer une surveillance, du fait, en particulier, que des évaluations des facteurs relatifs à la vie privée doivent être présentées au cours du processus de demande. De même, le processus réglementaire permet d'établir une liste publique précise des organismes désignés comme étant des organismes d'enquête en vertu de la Loi[14].

Le Comité appuie l'idée d'une exception aux principes visant le consentement, aux fins d'enquêtes en vertu de la LPRPDE. Nous jugeons inquiétant le manque de cohérence de l'article 7 de la Loi à cet égard et, dans un souci d'harmonisation, nous recommandons d'adopter l'approche suivie dans les Lois de l'Alberta et de la Colombie-Britannique en matière de protection des renseignements personnels dans le secteur privé. Ces Lois dites de « deuxième génération » autorisent la collecte, l'utilisation et la communication de renseignements personnels sans le consentement du principal

---

[14] Commissariat à la protection de la vie privée, *Examen, prévu par la loi, de la LPRPDE : Aperçu de la consultation du CPVP*, 27 novembre 2006.

améliorerait la capacité du Commissariat de bien saisir l'objet d'une plainte de façon à éviter que le recours aux exceptions ne devienne trop systématique. À cet égard, la commissaire a fourni un exemple d'une exception poussée à l'extrême, au point d'entraîner de l'ingérence dans la vie privée des employés qui étaient notamment assujettis à une surveillance au travail.

Le Comité convient que le principe énoncé dans la LPRPDE en ce qui concerne le consentement ne s'adapte pas facilement au contexte du travail, mais est toutefois conscient du fait que la création d'exceptions à l'exigence de consentement pour les relations entre employés et employeurs, ou l'établissement d'un code distinct relatif à l'emploi est une entreprise complexe. Nous recommandons donc que le gouvernement s'inspire des modèles actuellement en vigueur au Québec, en Colombie-Britannique et en Alberta pour élaborer une approche fédérale convenable qui permette la mise en œuvre d'un modèle viable qui ne nuira pas à la bonne marche des relations de travail et protégera la vie privée des employés.

Recommandation 5

Le Comité recommande que les lois du Québec, de l'Alberta et de la Colombie-Britannique en matière de protection des renseignements personnels dans le secteur privé soient prises en compte dans le but d'élaborer une modification qui pourrait être intégrée à la LPRPDE, pour tenir compte du contexte particulier dans lequel évoluent les employeurs et les employés régis par des lois fédérales.

B. Organismes d'enquête

La LPRPDE renferme deux dispositions qui permettent la communication à un organisme d'enquête de renseignements personnels à l'insu de l'intéressé et sans son consentement. l'alinéa 7(3)*d)* prévoit que cette communication peut être faite, à l'initiative de l'organisation, à un organisme d'enquête pour certaines fins précises, tandis que l'alinéa 7(3)(*h*.2) autorise un organisme d'enquête à communiquer des renseignements à des fins liées à une enquête sur la violation d'une entente ou la dérogation à une loi fédérale ou provinciale. Les organismes d'enquête sont désignés par règlement et ils sont actuellement au nombre de 75 environ.

La plupart des organisations commerciales que nous avons entendues estiment qu'il faudrait modifier la LPRPDE pour remédier aux problèmes liés à la nature et au fonctionnement des organismes d'enquête de même qu'au processus de désignation. Ainsi, certains témoins ont soutenu que les exceptions prévues à l'article 7 en ce qui concerne la collecte, l'utilisation et la communication comportent de nombreuses incohérences qui nuisent aux efforts déployés par les organisations pour détecter et prévenir la fraude. Voici ce qu'a dit à ce sujet l'Association des banquiers canadiens dans son mémoire au Comité :

Encore une fois, les Lois sur la protection des renseignements personnels de la Colombie-Britannique et de l'Alberta, qui abordent la question de l'emploi sous un autre angle, ont été évoquées. Le commissaire à l'information et la protection de la vie privée de la Colombie-Britannique, David Loukidelis, a expliqué au Comité l'approche adoptée par sa province :

> Une organisation de la Colombie-Britannique n'a pas à obtenir le consentement des employés pour recueillir, utiliser et communiquer ces renseignements. Les employeurs n'ont pas pour autant la liberté de faire n'importe quoi dans ce domaine, parce que la définition des renseignements personnels de l'employé précise qu'il s'agit exclusivement des renseignements qu'un employeur recueille à seule fin d'établir, de gérer ou de terminer une relation d'emploi avec une personne particulière. La définition exige en outre que la collecte, l'utilisation et la communication de ces renseignements se limitent à des fins raisonnables liées au travail accompli. La Colombie-Britannique a décidé de ne pas se fonder sur le consentement, reconnaissant que, dans le contexte de l'emploi, celui-ci est souvent imposé parce que l'employé est obligé d'accepter les pratiques de l'employeur, et qu'il ne convient pas, par exemple, de demander à un employeur d'obtenir le consentement d'un employé soupçonné de fraude avant de le soumettre à une surveillance. En effet, vous ne pouvez pas vous attendre à ce qu'une personne que vous soupçonnez de vous voler consente à être surveillée. Par conséquent, au lieu de choisir l'approche du consentement, la Colombie-Britannique a décidé de permettre la collecte, l'utilisation et la communication des renseignements personnels qui s'inscrivent dans la définition [...] (29 novembre 2006)

Au début de nos audiences, la commissaire à la protection de la vie privée avait exprimé des mises en garde à propos de l'idée d'adopter les approches retenues par l'Alberta et la Colombie-Britannique en matière de renseignements des employés. Tout en reconnaissant que les renseignements personnels des employés étaient à l'origine de certaines des plaintes les plus délicates qu'elle ait eues à traiter en vertu de la LPRPDE, la commissaire disait craindre que le fait de soustraire, à l'application du processus de consentement, une grande partie des renseignements personnels des employés risquait de priver ces mêmes employés de droits qui leur sont actuellement reconnus en vertu de la LPRPDE. À la fin de l'actuel processus d'examen, la commissaire nous a toutefois proposé une solution qui, selon elle, permettrait de remédier à toutes les préoccupations exprimées. Ainsi, elle préconise de s'inspirer du modèle albertain, à savoir un code relatif aux employés reposant sur le critère des fins raisonnables, et d'y intégrer aussi l'approche adoptée par le Québec pour protéger les renseignements personnels des employés. Ainsi, toute exception à l'égard des renseignements personnels devrait être assortie de l'obligation de respecter la dignité des employés et d'évaluer la situation pour voir s'il n'y a pas d'ingérence abusive dans la vie privée de l'employé.

La commissaire a tenu à préciser que l'établissement des détails du régime qu'elle propose ne sera pas une mince tâche; elle a toutefois proposé de se servir de l'article 7 de la Loi, qui prévoit des exceptions à l'égard de l'obligation d'obtenir le consentement des personnes intéressées avant de recueillir, d'utiliser et de communiquer des renseignements personnels, et d'y ajouter une disposition pour qu'il soit possible de se prévaloir de ces exceptions au moment d'établir ou de gérer une relation d'emploi ou d'y mettre fin. De l'avis de la commissaire, la prise en compte de la notion de dignité

Recommandation 4

Le Comité recommande d'envisager de modifier la LPRPDE pour y préciser les exigences applicables à la forme et à la conformité du consentement et établir une distinction entre les différentes formes de consentement : explicite, implicite et présumé/refusé. Il conviendrait, à cet égard, de se reporter aux Lois de l'Alberta et de la Colombie-Britannique en matière de protection des renseignements personnels.

2. Exceptions

A. Relations entre employeurs et employés

Comme il est mentionné au début du présent rapport, la LPRPDE établit les règles régissant la collecte, l'utilisation et la communication de renseignements personnels dans le secteur privé, mais seulement dans le cadre d'activités commerciales. Elle vise aussi à réglementer les renseignements personnels des employés mais, en raison de questions de compétence, elle s'applique uniquement aux emplois assujettis à la législation fédérale. Le problème qui a été soulevé devant le Comité est le suivant : un modèle de consentement conçu pour des entreprises commerciales peut-il s'appliquer dans le contexte de l'emploi?

L'ETCOF (Employeurs des transports et communications de régie fédérale) a vigoureusement fait valoir que l'actuel modèle de consentement applicable, en vertu de la LPRPDE, n'est pas adapté au milieu du travail. L'ETCOF a soulevé un certain nombre de questions relatives à l'emploi, dont certaines sont abordées ailleurs dans le rapport (p. ex., en ce qui concerne le produit du travail et les coordonnées des entreprises). La principale préoccupation de l'ETCOF porte toutefois sur le consentement. L'ETCOF est d'avis qu'il faudrait ajouter une définition de « renseignements personnels des employés » dans la LPRPDE et que l'utilisation, la collecte ou la communication raisonnable de renseignements relatifs à la gestion des relations de travail à des fins commerciales ne devrait pas exiger le consentement de l'employé. Voici les options proposées par l'ETCOF dans son mémoire au Comité :

> Plusieurs options s'offrent dans la façon de traiter le consentement d'un employé, y compris l'utilisation d'un consentement implicite ou tacite, ou même l'élimination de devoir obtenir le consentement d'un employé lorsqu'il s'agit de recueillir, d'utiliser ou de communiquer des renseignements personnels dans l'administration raisonnable des relations du travail (semblable à l'approche utilisée en C.-B. et en Alberta). Nous recommandons que les questions entourant le consentement d'un employé soient examinées et reconsidérées durant le processus de révision de la Loi. [traduction] (décembre 2006, p. 4)

dans *Le Petit Larousse illustrée 2002* ainsi que dans la 10e édition de *The Concise Oxford Dictionary*, nous recommandons que ces définitions soient prises en considération à cet égard.

Recommandation 3

Le Comité recommande qu'une définition de « destruction » soit ajoutée à la LPRPDE afin de guider les organisations sur la façon de bien détruire les documents papier et les fichiers électroniques.

CONSENTEMENT

1. Principes généraux

Le consentement est la pierre angulaire de la plupart des lois sur la protection des renseignements, et il en va de même de la LPRPDE. À quelques très rares exceptions, la Loi exige que quiconque recueille, utilise et communique des renseignements personnels dans le cadre d'activités commerciales, en informe le principal intéressé et obtienne son consentement. Le troisième principe du Code type sur la protection des renseignements personnels, lequel Code constitue l'annexe 1 de la Loi, énonce les règles régissant le consentement. Ces principes généraux semblent toutefois difficiles à concilier pour tenir compte des réalités commerciales et garantir, en même temps, aux consommateurs une protection suffisante de leurs renseignements personnels.

Les représentants des consommateurs et les défenseurs de la vie privée qui ont comparu devant nous ont fait valoir qu'il est extrêmement difficile de se servir de la formulation d'un document établi par consensus (le Code type de protection des renseignements personnels[11]) comme fondement d'une loi. Selon eux, le libellé des principes de consentement est trop vague et se prête, par conséquent, à tout un éventail d'interprétations qui ne nous éclairent guère sur les exigences effectives de la Loi. Dans son mémoire au Comité, le Centre pour la défense de l'intérêt public formule les observations suivantes :

> L'annexe 1 de la LPRPDE renferme un principe sur le consentement qui est rédigé dans un style large et détermine les paramètres généraux du consentement aux fins de la protection des renseignements personnels dans un contexte commercial; cependant, le texte de ce principe n'aide guère les entreprises et les consommateurs qui recherchent un énoncé définitif concernant la nature du consentement, le type de consentement qui est exigé en vertu de la Loi et la façon de l'obtenir.

---

11 Voir la note en bas de page 4.

Lors de sa comparution devant le Comité, le représentant de la National Association for Information Destruction (NAID) a proposé un certain nombre de recommandations afin d'assurer la destruction sûre des renseignements, qui trop souvent fait défaut d'après l'organisme. D'ailleurs, M. David Carey, de la NAID, a fourni au Comité des exemples pour confirmer la nécessité de préciser dans la Loi les mesures à prendre lorsque des renseignements sont détruits. Il résume la situation ainsi à l'intention du Comité :

> Il ne faudrait pas beaucoup de temps pour trouver, n'importe quand, des renseignements personnels qui ont été jetés, qui sont intacts et accessibles au public. Le fait qu'on s'en débarrasse de façon imprudente, en les jetant dans des bennes à rebuts ou dans des poubelles, en est l'exemple évident. Il ne faut pas oublier non plus que le recyclage à lui seul ne constitue pas une destruction sûre des renseignements. Il est possible que les documents demeurent intacts pendant longtemps et puissent faire l'objet d'un manquement au respect de la vie privée avant qu'ils ne soient recyclés. La protection de la vie privée n'est plus simplement une question de droit de la personne. Une violation des droits des autres, en jetant aux rebuts nonchalamment leurs renseignements personnels, contribue considérablement à ce qui est devenu une épidémie mondiale de vols d'identité. Selon une étude qui a été faite aux États-Unis, la vaste majorité des vols d'identité est attribuable à l'accès aux renseignements personnels grâce à des moyens de faible technicité, comme fouiller dans des bennes à rebuts. (8 février 2007)

Le représentant de la NAID recommande par conséquent d'ajouter à la LPRPDE la définition suivante de « destruction » :

> Aux fins du principe 4.5 de l'annexe 1, on entend par destruction la destruction physique des dossiers de façon à rendre impossible la récupération de l'information (en tout ou en partie). Détruire signifie altérer jusqu'à faire disparaître. (NAID Canada, lettre datée du 21 février 2007)

Dans le mémoire qu'il a présenté au Comité[10], le ministère des Services gouvernementaux de l'Ontario a insisté sur l'importance d'informer les organisations sur la destruction protégée des renseignements personnels. Étant donné la fréquence des vols d'identité au Canada, le Ministère a recommandé que la commissaire donne plus d'indications dans ce domaine et précise les mesures que doivent prendre les organisations afin de détruire les documents papier et les fichiers électroniques de manière à ce que les renseignements personnels soient irrémédiablement détruits ou effacés.

Le Comité pense aussi que la destruction en bonne et due forme des renseignements personnels fait partie intégrante de tout régime de protection de ces renseignements. En fait, l'absence, dans la Loi, d'exigences claires en matière de destruction, risque de compromettre les mesures de protection de la vie privée intégrées à la LPRPDE. Nous recommandons par conséquent qu'une définition de « destruction » soit ajoutée à la LPRPDE afin de guider les organisations sur la façon de bien détruire les documents papier et les fichiers électroniques. Ayant examiné la définition de destruction

---

10 Décembre 2006.

renseignements personnels et régler au cas par cas les questions traitant le produit du travail. Elle a ajouté que l'adoption du code relatif aux employés qu'elle propose dans le cadre de la LPRPDE[9] permettrait de résoudre de nombreuses questions liées au produit du travail sans pour autant menacer les autres droits à la protection de la vie privée en milieu de travail.

Le Comité reconnaît que la question du produit du travail ne concerne pas un secteur en particulier, mais touche plutôt tout l'éventail des activités commerciales et professionnelles. Le Comité croit qu'il est nécessaire d'apporter des précisions dans le cadre de la LPRPDE quant à ce qui constitue un produit du travail par opposition aux renseignements personnels. Bien que nous hésitions à recommander un libellé particulier, étant donné les discussions que suscite la question, nous recommandons néanmoins de tenir compte de la définition de la Colombie-Britannique et de celle proposée par IMS, ainsi que l'approche adoptée par le Québec en matière de renseignements personnels sur les professionnels.

Recommandation 2

Le Comité recommande que la LPRPDE soit modifiée pour y inclure une définition du « produit du travail » qui précise explicitement que ce dernier ne constitue pas des renseignements personnels aux fins de la Loi. La définition devrait s'inspirer de la définition des « renseignements sur le produit du travail » contenue dans la Loi sur la protection des renseignements personnels de la Colombie-Britannique, de la définition proposée au Comité par IMS Canada et de l'approche adoptée au Québec dans la *Loi sur la protection des renseignements personnels dans le secteur privé* à l'égard des renseignements personnels de professionnels.

2. Destruction

Le principe 5 à l'annexe 1 de la LPRPDE porte sur la conservation des renseignements personnels. Essentiellement, les renseignements personnels ne doivent être conservés que le temps nécessaire à la réalisation des fins pour lesquelles ils sont recueillis. Il faudrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins pour lesquelles ils ont été recueillis, selon les politiques établies par l'organisation pour la destruction des renseignements personnels (principe 4.5.3). Le principe 7 de l'annexe exige que des mesures de sécurité protègent les renseignements personnels au moment de leur retrait ou de leur destruction afin d'empêcher les personnes non autorisées d'y avoir accès (principe 4.7.5).

---

9 Voir, dans la section Consentement du rapport, la partie portant sur les relations entre les employeurs et les employés.

particulièrement IMS — ne constituent pas des renseignements personnels aux fins de la LPRPDE, IMS souhaite néanmoins, pour dissiper tout doute, que la décision de la commissaire soit codifiée. L'entreprise propose le libellé suivant :

> les « renseignements sur le produit du travail » sont les renseignements préparés, recueillis ou communiqués par une personne ou un groupe de personnes dans le cadre de leurs fonctions. Ils ne comprennent pas :
>
> i) les renseignements personnels concernant une personne qui n'a ni préparé, ni recueilli, ni communiqué les renseignements;
>
> ii) les renseignements recueillis, utilisés ou communiqués à des fins de surveillance du milieu de travail. (8 février 2007, mémoire)

Pour ce qui est de savoir si les renseignements sur les ordonnances des médecins constituent un produit du travail en application de la LPRPDE, l'Association médicale canadienne (AMC) est d'avis qu'ils constituent les renseignements personnels du médecin au même titre que les autres données sur la pratique, et que les médecins ont des préoccupations légitimes quant à la protection de la vie privée et à l'utilisation de l'information par des tiers à des fins commerciales. L'AMC a recommandé que la LPRPDE soit modifiée afin d'inclure les données des médecins dans les renseignements personnels, mais elle a aussi mentionné la *Loi sur la protection des renseignements personnels dans le secteur privé* en vigueur au Québec, qui impose une surveillance réglementaire et donne aux particuliers le droit de s'exclure de la collecte, de l'utilisation et de la divulgation de renseignements personnels de professionnels.

L'approche du Québec est considérée comme une sorte de compromis puisque les renseignements sur le produit du travail de professionnels sont considérés comme se situant entre les renseignements personnels et les renseignements non personnels. La Loi autorise la divulgation, sans consentement, de renseignements personnels sur des professionnels se rapportant à leurs activités professionnelles; cependant, cette divulgation doit absolument se faire avec l'autorisation de la Commission du Québec puis sous sa surveillance (en consultation avec l'organisme de réglementation compétent). De plus, le professionnel doit avoir la possibilité de s'opposer à ce que ses renseignements soient utilisés aux fins projetées et il doit être informé régulièrement de ces fins. La personne autorisée à recevoir ces renseignements doit aussi faire rapport chaque année à la Commission de la mise en œuvre de l'autorisation, et la Commission doit publier dans son rapport annuel une liste des personnes autorisées[8].

La commissaire fédérale à la protection de la vie privée a maintenu tout au long des audiences que la question était difficile à régler; en d'autres mots, il n'existe pas de solution rapide ni de modèle clair à adopter. Elle préfère conserver la définition actuelle des

---

[8] *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q.ch. P-39.1, art. 21.1

> Dans une économie compétitive — et nous savons que le Parlement veut que notre économie soit compétitive —, il est essentiel que les sociétés aient accès aux renseignements relatifs aux produits et aux services qu'elles achètent à d'autres entreprises, de manière à pouvoir les utiliser pour innover et améliorer les produits et services qu'elles offrent elles-mêmes à leurs clients. Sans accès aux renseignements relatifs au produit du travail, on freinerait l'innovation et la concurrence dans l'économie. (6 février 2007)

Les entreprises appuient presque sans réserve l'approche adoptée dans le *Personal Information Protection Act* de la Colombie-Britannique, qui fait une distinction entre les renseignements sur le produit du travail et les renseignements personnels. Selon l'article 1 de la Loi de la Colombie-Britannique, les renseignements sur le produit du travail désignent les renseignements préparés ou recueillis par une personne ou un groupe de personnes dans le cadre de leurs fonctions; ils ne comprennent pas les renseignements personnels concernant une personne qui n'a ni préparé ni recueilli les renseignements. La plupart des entreprises favorisent cette définition qui mettrait fin aux incertitudes grâce à une application uniforme.

Dans le mémoire qu'il a présenté au Comité, le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, David Loukidelis, souligne les difficultés d'interprétation et d'application qui peuvent survenir si une loi sur la protection de la vie privée ne fait pas de distinction entre les renseignements personnels qui concernent un individu et les renseignements que cette personne produit ou réunit dans le cadre de son travail, de ses fonctions ou de ses activités. Toutefois, quand les membres du Comité l'ont interrogé à ce sujet, il a répondu comme suit :

> Comme je l'ai mentionné, la Loi de la Colombie-Britannique comporte une définition de l'information sur le produit du travail. Notre Assemblée législative m'a donc donné un libellé clair sur lequel je peux baser mon travail. Si une affaire m'est transmise sous forme d'une demande officielle de renseignements, je dois procéder au cas par cas pour interpréter et appliquer les dispositions adoptées par notre Assemblée. Cela étant dit, sans cette définition, nous aurions dû nous contenter de la définition de « renseignements personnels », c'est-à-dire « tout renseignement concernant un individu identifiable », et affronter les mêmes difficultés que mes collègues fédéraux et les autres provinces, qui doivent se fonder sur leur loi relative au secteur public pour essayer de déterminer quels renseignements « concernent » un individu dans l'esprit du législateur, et aboutir peut-être au même résultat. (29 novembre 2006)

La question du « produit du travail » revêt un intérêt particulier en matière de renseignements sur la santé. IMS Canada, un important fournisseur de renseignements, de données statistiques et d'analyses dans le secteur de la santé, voudrait une définition du « produit du travail », qui se rapproche de celle établie par la Colombie-Britannique, mais qui cherche également à répondre à certaines des préoccupations de la commissaire à la protection de la vie privée; en effet, celle-ci craint qu'une définition ou une interprétation plus large du terme englobe par inadvertance la surveillance du milieu de travail. Même si la commissaire a déjà statué que les données sur les habitudes des médecins en matière d'établissement d'ordonnances — données qui intéressent tout

La commissaire à la protection de la vie privée a attiré l'attention du Comité sur l'approche prise dans le *Personal Information Protection Act* de l'Alberta. Elle trouve intéressante la définition contenue dans cette Loi de protection générale de la vie privée parce qu'elle est suffisamment générale, mais aussi parce qu'elle restreint les fins pour lesquelles de tels renseignements peuvent être recueillis, utilisés ou communiqués.

L'alinéa 1*a*) de la loi de l'Alberta définit les « coordonnées des entreprises » comme étant le nom, le poste ou le titre de la personne, le numéro de téléphone, l'adresse, l'adresse électronique et le numéro de télécopieur et d'autres renseignements semblables concernant l'entreprise. L'alinéa 4(3)*d*) de la Loi constitue une disposition d'exception qui stipule que la loi ne s'applique pas aux coordonnées d'entreprise lorsque celles-ci sont recueillies, utilisées ou communiquées dans le but d'entrer en contact avec une personne en sa qualité d'employée ou de représentante d'une organisation, et uniquement dans ce but.

Le Comité estime que les dispositions de protection contenues dans la LPRPDE ne devraient pas s'appliquer aux coordonnées des entreprises et que ces coordonnées ne doivent pas être limitées à la technologie de l'information existante à un moment précis. Il faut, par conséquent, mettre à jour la LPRPDE afin que figurent dans les coordonnées les adresses électroniques et les numéros de télécopieur des entreprises, ainsi que les innovations à venir en matière de communication commerciale. À l'instar de la commissaire à la protection de la vie privée, nous préconisons l'approche de l'Alberta et formulons la recommandation suivante.

Recommandation 1

Le Comité recommande qu'une définition des coordonnées des entreprises soit ajoutée à la LPRPDE et que soient prises en considération, à cette fin, la définition et la disposition limitative connexe qui se trouvent dans la Loi sur la protection des renseignements personnels de l'Alberta.

B. Produit du travail

De nombreux employeurs, des entreprises et des fournisseurs de renseignements sur la santé ont souligné la distinction qu'il faut faire entre les renseignements personnels concernant une personne et les renseignements générés dans le cadre d'activités professionnelles ou commerciales, ou liées à l'emploi. De nombreuses entreprises craignent que l'innovation et la croissance économique soient compromises si les travailleurs peuvent traiter les données au sujet du produit de leur travail ou des stratégies d'entreprises comme des renseignements personnels, en vertu de la LPRPDE. Mark Yakabuski, du Bureau d'assurance du Canada, s'exprime ainsi :

En vertu de l'article 11 de la Loi, la commissaire à la protection de la vie privée peut elle-même prendre l'initiative d'une plainte si elle a des motifs raisonnables de croire qu'une enquête devrait être menée sur une question relative à l'application de la Loi. Elle peut demander à la Cour fédérale d'examiner une plainte dont elle a pris l'initiative ou celle d'un plaignant, avec son consentement. Conformément à l'article 18 de la Loi, la commissaire à la protection de la vie privée a aussi le pouvoir de procéder à la vérification des pratiques de l'organisation en matière de gestion des renseignements personnels, si elle a des motifs raisonnables de croire que l'organisation a contrevenu aux dispositions de la Loi touchant la protection de ces renseignements, ou qu'elle n'applique pas une recommandation énoncée dans le Code type de la CSA.

L'article 28 de la LPRPDE crée des infractions pour les cas où une personne entrave l'action de la commissaire, dans le cadre d'un examen ou d'une vérification; détruit des documents visés par une demande de communication avant que tous les recours prévus par la Loi aient été épuisés; ou congédie, suspend ou rétrograde un employé qui révèle que son employeur a contrevenu à la Loi.

DÉFINITIONS

1. Renseignement personnel

A. Coordonnées des entreprises

Le paragraphe 2(1) de la LPRPDE définit le « renseignement personnel », aux fins de la Loi, comme étant « tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresses et numéro de téléphone de son lieu de travail ». Ainsi, les coordonnées des entreprises sont soustraites à la protection afin que les clients des organisations et d'autres puissent communiquer facilement avec les employés. La *Loi fédérale sur la protection des renseignements personnels* prévoit des dispositions semblables à l'égard des fonctionnaires.

Plusieurs organisations ont demandé d'élargir la définition de façon à tenir compte, dans les coordonnées des entreprises soustraites à l'application de la Loi, des moyens que les organisations utilisent à notre époque pour communiquer avec leurs clients. Il a ainsi été suggéré d'inscrire dans la Loi une définition des « coordonnées des entreprises », qui comprendrait tous les types de renseignements communiqués dans le contexte commercial et qui ne serait pas limitée à une technologie particulière. Ainsi, les coordonnées des entreprises devraient comprendre les numéros de télécopieur et les adresses de courriel, en plus d'autres renseignements semblables.

cas où une organisation peut recueillir, utiliser ou communiquer des renseignements personnels à l'insu de l'intéressé et sans son consentement; à cet égard, il est essentiel au fonctionnement du régime de protection de la vie privée établi par la Loi[5].

La LPRPDE donne aux particuliers le droit de prendre connaissance des renseignements personnels qui les concernent et d'y faire apporter des corrections, au besoin. Une organisation doit répondre aux demandes d'accès à ces renseignements dans les 30 jours, mais elle peut demander plus de temps dans certaines situations. Elle peut refuser de communiquer les renseignements à l'intéressé si la communication révèle un renseignement personnel relatif à un tiers qui ne peut être retranché d'un document. Cette interdiction est toutefois levée si le tiers consent à la communication ou si l'intéressé a besoin du renseignement parce que sa vie, sa santé ou sa sécurité est en danger. Une organisation peut par ailleurs refuser l'accès à des renseignements personnels lorsque ceux-ci sont protégés par le secret professionnel qui lie l'avocat à son client ou que la communication révélerait des renseignements commerciaux confidentiels[6]. La communication est toutefois autorisée si la personne a besoin des renseignements parce que sa vie, sa santé ou sa sécurité est menacée.

La LPRPDE est administrée selon un modèle d'ombudsman semblable à celui que l'on trouve dans la *Loi sur la protection des renseignements personnels* et dans la *Loi sur l'accès à l'information*. Un particulier peut adresser une plainte à la commissaire fédérale à la protection de la vie privée au sujet de la conformité d'une organisation à la loi ou au Code de la CSA[7], auquel cas la commissaire tentera habituellement de résoudre l'affaire par la persuasion et la négociation. Si cette approche ne réussit pas, la commissaire a le pouvoir d'assigner des témoins, de faire prêter serment et de contraindre des personnes à produire des documents afin de se prononcer sur l'affaire. Elle doit exposer ses conclusions dans un rapport dans un délai d'un an suivant le dépôt de la plainte. Les conclusions de la commissaire ne lient pas les parties et elles n'ont pas non plus de force persuasive devant la Cour fédérale. Après avoir reçu le rapport de la commissaire, le plaignant a toutefois le droit d'exercer des recours judiciaires et de réclamer une ordonnance de conformité et des dommages-intérêts, auprès de la Cour fédérale.

---

5 Par exemple, des renseignements personnels peuvent être *recueillis* à l'insu de l'intéressé et sans son consentement à des fins d'application de la loi, lorsque la collecte est dans l'intérêt supérieur de l'intéressé, qu'elle est faite à des fins journalistiques, artistiques ou littéraires; ou qu'il s'agit d'un renseignement auquel le public a accès. Des renseignements personnels peuvent être *utilisés* à l'insu de l'intéressé et sans son consentement pour des raisons semblables, ainsi qu'à des fins de recherche dans certains cas au su de la commissaire à la protection de la vie privée. Enfin, des renseignements personnels peuvent être *communiqués* à l'insu de l'intéressé et sans son consentement aux fins de l'application de la loi et de la sécurité nationale, dans des situations d'urgence, ainsi qu'à des fins de recherche et d'archives.

6 Ces exemptions reflètent, en grande partie, celles que l'on trouve dans la *Loi sur l'accès à l'information* et fournissent un exemple de la nature complémentaire des régimes de protection des renseignements personnels et d'accès à l'information.

7 Article 11.

La LPRPDE est entrée en vigueur en trois phases :

- Depuis le 1er janvier 2001, la Loi s'applique aux industries du secteur privé de compétence fédérale (comme les télécommunications, la radiodiffusion, les institutions financières, les transports interprovinciaux et les compagnies aériennes). Elle s'applique aussi au commerce interprovincial ou international de renseignements personnels.

- Depuis le 1er janvier 2002, la Loi s'applique aussi aux renseignements personnels sur la santé.

- Depuis le 1er janvier 2004, les dispositions de la Loi s'appliquent plus largement à toutes les organisations d'une province, même si elles recueillent, utilisent ou communiquent des renseignements personnels seulement dans la province. Toutefois, peuvent être exemptées les organisations ou les activités dans les provinces qui ont adopté une loi sur la protection de la vie privée semblable à la loi fédérale. Jusqu'à maintenant, seuls le Québec, l'Alberta, l'Ontario (en matière de renseignements personnels sur la santé) et la Colombie-Britannique se sont dotés de lois provinciales jugées essentiellement similaires à la LPRPDE.

Une fois qu'une organisation est visée par la LPRPDE, l'article 5 l'oblige à se conformer aux obligations énoncées dans le Code type de l'Association canadienne de normalisation (CSA) (annexe 1 de la Loi)[4], sous réserve des exemptions prévues aux articles 6 à 9. L'article 5 précise par ailleurs que l'emploi du conditionnel dans l'annexe 1 indique qu'il s'agit non pas d'une obligation mais d'une recommandation. Le paragraphe 5(3) prévoit en outre un critère dit des « fins acceptables », selon lequel les fins auxquelles une organisation peut recueillir, utiliser ou communiquer des renseignements personnels doivent se limiter à celles « qu'une personne raisonnable estimerait acceptables dans les circonstances ». L'article 7 énonce un certain nombre de

---

[4] Au début des années 1990, devant l'absence de normes nationales de protection des données au Canada, un comité composé de représentants des consommateurs, de l'entreprise, du gouvernement et des syndicats a élaboré, sous les auspices de l'Association canadienne de normalisation (CSA), un ensemble de principes de protection de la vie privée que le Conseil canadien des normes a approuvé en 1996 à titre de normes nationales. Le *Code type sur la protection des renseignements personnels* de la CSA établit dix principes conçus pour servir aux entreprises de guide de pratiques équitables en matière de renseignements. Le libellé du Code a fini par être intégré à la LPRPDE, sous forme d'annexe de la Loi. Pour en connaître davantage sur le Code de la CSA et son intégration à la LPRPDE, voir *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* by Perrin, Black, Flaherty and Rankin, Irwin Law Inc., Toronto, 2001.

Nous sommes conscients de la nécessité de consacrer davantage de ressources aux mesures visant à sensibiliser les particuliers et les organisations aux droits et aux responsabilités que leur confère la LPRPDE. Des témoins nous ont affirmé que la plupart des Canadiens sont généralement peu au fait de leurs droits en matière de protection de la vie privée et le sont encore moins en ce qui concerne, en particulier, les droits conférés par la LPRPDE. Nous nous sommes aussi laissé dire que l'un des principaux obstacles qui se posent à la plupart des petites et moyennes entreprises réside dans la difficulté de comprendre leurs obligations en vertu de la Loi. À notre avis, le succès des modifications que nous proposons d'apporter à la LPRPDE, et en définitive de la Loi elle-même, se mesurera, en bout de ligne, à la capacité des particuliers de faire des choix éclairés au sujet de leurs renseignements personnels et à la capacité des organisations de pleinement comprendre leurs obligations en vertu de la Loi. Étant donné qu'il est clairement du ressort du Commissariat à la protection de la vie privée de sensibiliser la population et d'inciter les organisations visées par la loi à s'y conformer, nous espérons que le travail en ce sens continuera de s'intensifier et que le gouvernement mettra lui aussi tout en œuvre pour atteindre ces objectifs avec le concours des organisations concernées et de la commissaire à la protection de la vie privée.

APERÇU DE LA LOI

Sous réserve de certaines exemptions qui y sont prévues[1], la LPRPDE s'applique aux organisations du secteur privé qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre d'activités commerciales. Elle s'applique également à la collecte, à l'utilisation et à la communication de renseignements personnels relatifs aux employés d'organisations sous réglementation fédérale[2]. Le paragraphe 2(1) de la Loi définit les renseignements personnels au sens large comme « tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail ». Dans le but évident d'englober une gamme étendue de transactions, l'article 2 définit par ailleurs « activité commerciale » comme étant « toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial de par leur nature, y compris la vente, le troc ou la location de listes de donneurs, d'adhésion ou de collecte de fonds[3] ».

---

1 La Loi ne s'applique pas aux institutions fédérales visées par la *Loi sur la protection des renseignements personnels*; aux renseignements personnels recueillis, utilisés ou communiqués par un individu uniquement à des fins personnelles ou domestiques; ni à une organisation à l'égard des renseignements personnels qu'elle recueille, utilise ou communique uniquement à des fins journalistiques, artistiques ou littéraires (paragr. 4(2)).

2 Nonobstant la compétence provinciale à l'égard des relations de travail, le gouvernement fédéral peut réglementer les renseignements concernant les employés, mais uniquement par rapport aux installations, ouvrages, entreprises et secteurs d'activité soumis à l'autorité législative du Parlement fédéral.

3 La LPRPDE s'applique uniquement aux activités commerciales parce que les provinces ont compétence exclusive en matière de propriété privée et de droits civils. Le gouvernement fédéral a donc décidé de légiférer dans ce domaine en vertu de son pouvoir général de réglementer le commerce.

INTRODUCTION

Conformément à l'article 29 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) et à l'ordre de renvoi de la Chambre des communes, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (le Comité) a tenu des audiences sur l'application de la Partie 1, Protection des renseignements personnels dans le secteur privé, de la Loi. Entre le 20 novembre 2006 et le 22 février 2007, il a entendu 67 témoins et reçu 34 mémoires d'autres particuliers et organismes.

Tous nos témoins sont généralement favorables à l'existence d'une loi fédérale pour protéger les renseignements personnels dans le secteur privé, compte tenu en particulier de la rapidité d'expansion de l'actuelle myriade de technologies de l'information et de leur capacité de transcender les frontières nationales. Dans ce contexte, la question au cœur du débat est celle-ci : comment pouvons-nous, de la meilleur façon, concilier dans la Loi les exigences liées à la protection de la vie privée des particuliers (ce qu'on sait à leur sujet et qui le sait) et les besoins légitimes des organisations commerciales relativement à la gestion de leurs fonds de renseignements?

Le présent rapport ne recommande pour l'instant aucune modification radicale de la LPRPDE. Étant donné que la Loi n'est pleinement entrée en vigueur qu'en janvier 2004 (voir plus loin l'Aperçu de la Loi), le Comité est conscient que tous les différents aspects de sa mise en œuvre ne se sont peut-être pas encore entièrement concrétisés. Par conséquent, même si nous avons entendu des témoignages sur de nombreuses questions, nous n'avons abordé que celles qui, selon nous, devaient être examinées maintenant.

Les recommandations du présent rapport proposent essentiellement des modifications mineures justifiées, pour la plupart, par la nécessité de mieux harmoniser la loi fédérale aux lois du Québec, de l'Alberta et de la Colombie-Britannique en matière de protection des renseignements personnels dans le secteur privé, lesquelles lois sont toutes essentiellement similaires. En fait, des défenseurs de la vie privée, des universitaires, des organisations commerciales et industrielles, de même que la commissaire fédérale à la protection de la vie privée, nous ont tous affirmé qu'il fallait se servir de ces lois provinciales comme points de référence pour modifier la LPRPDE. Ainsi, certains ont fait valoir qu'étant donné que les lois de l'Alberta et de la Colombie-Britannique ont été rédigées après les lois fédérale et québécoise, ces provinces ont l'avantage d'avoir pu mettre à profit l'expérience du Québec et du gouvernement fédéral pour apporter des améliorations à leurs lois respectives. Des témoins ont soutenu que ces lois dites « de deuxième génération » présentent une vision plus pragmatique et moderne de la protection des renseignements personnels dans le contexte d'aujourd'hui.

TABLE DES MATIÈRES

COMITÉ PERMANENT L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

a l'honneur de présenter son

QUATRIÈME RAPPORT

Conformément au mandat que lui confère l'article 108(2) du Règlement, le Comité a étudié, un Examen, prévu par la loi, de la Loi sure la protection des renseignements personnels et les documents électroniques (LPRPDÉ) et a adopté le rapport suivant :

COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

PRÉSIDENT

Tom Wappel

VICE-PRÉSIDENTS

Pat Martin
David Tilson

MEMBRES

Sukh Dhaliwal
Glen Pearson
Scott Reid
Dave Van Kesteren
Mike Wallace
Carole Lavallée
Jim Peterson
Bruce Stanton
Robert Vincent

GREFFIER DU COMITÉ

Richard Rumas

BIBLIOTHÈQUE DU PARLEMENT
Service d'information et de recherche parlementaires

Kristen Douglas

Nancy Holmes

EXAMEN, PRÉVU PAR LA LOI, DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES (LPRDÉ)

Quatrième Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le président

Tom Wappel, député

Mai 2007

39e LÉGISLATURE, 1re SESSION

En vente : Communication Canada — Édition, Ottawa, Canada K1A 0S9

CHAMBRE DES COMMUNES
CANADA

EXAMEN, PRÉVU PAR LA LOI, DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUE (LPRPDÉ)

Quatrième Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le président

Tom Wappel, député

Mai 2007

39e LÉGISLATURE, 1re SESSION